

117TH CONGRESS
2D SESSION

H. R. 8152

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

IN THE HOUSE OF REPRESENTATIVES

JUNE 21, 2022

Mr. PALLONE (for himself, Mrs. RODGERS of Washington, Ms. SCHAKOWSKY, and Mr. BILIRAKIS) introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “American Data Privacy and Protection Act”.

6 (b) TABLE OF CONTENTS.—The table of contents of
7 this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Definitions.

TITLE I—DUTY OF LOYALTY

- Sec. 101. Data minimization.
- Sec. 102. Loyalty duties.
- Sec. 103. Privacy by design.
- Sec. 104. Loyalty to individuals with respect to pricing.

TITLE II—CONSUMER DATA RIGHTS

- Sec. 201. Consumer awareness.
- Sec. 202. Transparency.
- Sec. 203. Individual data ownership and control.
- Sec. 204. Right to consent and object.
- Sec. 205. Data protections for children and minors.
- Sec. 206. Third-party collecting entities.
- Sec. 207. Civil rights and algorithms.
- Sec. 208. Data security and protection of covered data.
- Sec. 209. Small business protections.
- Sec. 210. Unified opt-out mechanisms.

TITLE III—CORPORATE ACCOUNTABILITY

- Sec. 301. Executive responsibility.
- Sec. 302. Service providers and third parties.
- Sec. 303. Technical compliance programs.
- Sec. 304. Commission approved compliance guidelines.
- Sec. 305. Digital content forgeries.

TITLE IV—ENFORCEMENT, APPLICABILITY, AND MISCELLANEOUS

- Sec. 401. Enforcement by the Federal Trade Commission.
- Sec. 402. Enforcement by State attorneys general.
- Sec. 403. Enforcement by individuals.
- Sec. 404. Relationship to Federal and State laws.
- Sec. 405. Severability.
- Sec. 406. COPPA.
- Sec. 407. Authorization of appropriations.
- Sec. 408. Effective date.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **AFFIRMATIVE EXPRESS CONSENT.**—

4 (A) **IN GENERAL.**—The term “affirmative
5 express consent” means an affirmative act by
6 an individual that clearly communicates the in-
7 dividual’s freely given, specific, informed, and
8 unambiguous authorization for an act or prac-
9 tice, in response to a specific request from a

covered entity that meets the requirements of subparagraph (B).

(B) REQUEST REQUIREMENTS.—The requirements of this subparagraph with respect to a request from a covered entity to an individual are the following:

(i) The request is provided to the individual in a clear and conspicuous standalone disclosure made through the primary medium used to offer the covered entity's product or service.

(ii) The request includes a description of the act or practice for which the individual's consent is sought and—

(I) clearly states the specific categories of covered data that the covered entity shall collect, process, and transfer for each act or practice;

(II) clearly distinguishes between any act or practice which is necessary to fulfill a request of the individual and any act or practice which is for another purpose; and

(III) includes a prominent heading and is written in easy-to-under-

1 stand language that would enable a
2 reasonable individual to identify and
3 understand the processing purpose for
4 which consent is sought and the cov-
5 ered data to be collected, processed, or
6 transferred by the covered entity for
7 such processing purpose.

8 (iii) The request clearly explains the
9 individual's applicable rights related to
10 consent.

11 (iv) The request shall be made in a
12 manner readily accessible to and usable by
13 individuals with disabilities.

14 (v) The request shall be made avail-
15 able to the public in each language in
16 which the covered entity provides a product
17 or service for which authorization is sought
18 or in which the covered entity carries out
19 any activity related to any product or serv-
20 ice for which the covered data of the indi-
21 vidual may be collected, processed, or
22 transferred.

23 (C) EXPRESS CONSENT REQUIRED.—A
24 covered entity shall not infer that an individual
25 has provided affirmative express consent to an

1 act or practice from the inaction of the indi-
2 vidual or the individual's continued use of a
3 service or product provided by the covered enti-
4 ty.

5 (D) PRETEXTUAL CONSENT PROHIB-
6 ITED.—A covered entity shall not obtain or at-
7 tempt to obtain the affirmative express consent
8 of an individual through—

9 (i) the use of any false, fictitious,
10 fraudulent, or materially misleading state-
11 ment or representation; or

12 (ii) the design, modification, or ma-
13 nipulation of any user interface with the
14 purpose or substantial effect of obscuring,
15 subverting, or impairing a reasonable indi-
16 vidual's autonomy, decision making, or
17 choice to provide such consent or any cov-
18 ered data.

19 (2) ALGORITHM.—The term “algorithm” means
20 a computational process that uses machine learning,
21 natural language processing, artificial intelligence
22 techniques, or other computational processing tech-
23 niques of similar or greater complexity that makes
24 a decision or facilitate human decision making with
25 respect to covered data, including to determine the

1 provision of products or services or to rank, order,
2 promote, recommend, amplify, or similarly determine
3 the delivery or display of information to an indi-
4 vidual.

5 (3) BIOMETRIC INFORMATION.—

6 (A) IN GENERAL.—The term “biometric
7 information” means any covered data generated
8 from the technological processing of an individ-
9 ual’s unique biological, physical, or physiological
10 characteristics that is linked or reasonably
11 linkable to an individual including—

12 (i) fingerprints;

13 (ii) voice prints;

14 (iii) iris or retina scans;

15 (iv) facial mapping or hand mapping,
16 geometry, or templates; or

17 (v) gait or personally identifying phys-
18 ical movements.

19 (B) EXCLUSION.—The term “biometric in-
20 formation” does not include—

21 (i) a digital or physical photograph;

22 (ii) an audio or video recording; or

23 (iii) data generated from a digital or
24 physical photograph, or an audio or video

1 recording that cannot be used to identify
2 an individual.

3 (4) COLLECT; COLLECTION.—The terms “col-
4 lect” and “collection” mean buying, renting, gath-
5 ering, obtaining, receiving, accessing, or otherwise
6 acquiring covered data by any means.

7 (5) COMMISSION.—The term “Commission”
8 means the Federal Trade Commission.

9 (6) COMMON BRANDING.—The term “common
10 branding” means a name, service mark, or trade-
11 mark that is shared by 2 or more entities.

12 (7) CONTROL.—The term “control” means,
13 with respect to an entity—

14 (A) ownership of, or the power to vote,
15 more than 50 percent of the outstanding shares
16 of any class of voting security of the entity;

17 (B) control over the election of a majority
18 of the directors of the entity (or of individuals
19 exercising similar functions); or

20 (C) the power to exercise a controlling in-
21 fluence over the management of the entity.

22 (8) COVERED DATA.—

23 (A) IN GENERAL.—The term “covered
24 data” means information that identifies or is
25 linked or reasonably linkable, alone or in com-

1 bination with other information, to an indi-
2 vidual or a device that identifies or is linked or
3 reasonably linkable to an individual, and may
4 include derived data and unique identifiers.

5 (B) EXCLUSIONS.—The term “covered
6 data” does not include—

- 7 (i) de-identified data;
- 8 (ii) employee data;
- 9 (iii) publicly available information; or
- 10 (iv) inferences made exclusively from
11 multiple independent sources of publicly
12 available information that do not reveal
13 sensitive covered data with respect to an
14 individual.

15 (C) EMPLOYEE DATA DEFINED.—For pur-
16 poses of subparagraph (B), the term “employee
17 data” means—

- 18 (i) information relating to a job appli-
19 cant collected by a covered entity acting as
20 a prospective employer of such job appli-
21 cant in the course of the application, or
22 hiring process, provided that such informa-
23 tion is collected, processed, or transferred
24 by the prospective employer solely for pur-
25 poses related to the employee’s status as a

1 current or former job applicant of such
2 employer;

3 (ii) the business contact information
4 of an employee, including the employee's
5 name, position or title, business telephone
6 number, business address, or business
7 email address that is provided to an em-
8 ployer by an employee who is acting in a
9 professional capacity, provided that such
10 information is collected, processed, or
11 transferred solely for purposes related to
12 such employee's professional activities;

13 (iii) emergency contact information
14 collected by an employer that relates to an
15 employee of that employer, provided that
16 such information is collected, processed, or
17 transferred solely for the purpose of having
18 an emergency contact on file for the em-
19 ployee; or

20 (iv) information relating to an em-
21 ployee (or a spouse, dependent, other cov-
22 ered family member, or beneficiary of such
23 employee) that is necessary for the em-
24 ployer to collect, process, or transfer solely
25 for the purpose of administering benefits

1 to which such employee (or spouse, de-
2 pendent, other covered family member, or
3 beneficiary of such employee) is entitled on
4 the basis of the employee's position with
5 that employer.

6 (9) COVERED ENTITY.—

7 (A) The term “covered entity”—

8 (i) means any entity or any person,
9 other than an individual acting in a non-
10 commercial context, that alone or jointly
11 with others determines the purposes and
12 means of collecting, processing, or trans-
13 ferring covered data and—

14 (I) is subject to the Federal
15 Trade Commission Act (15 U.S.C. 41
16 et seq.);

17 (II) is a common carrier subject
18 to the Communications Act of 1934
19 (47 U.S.C. 151 et seq.) and all Acts
20 amendatory thereof and supple-
21 mentary thereto title II of the Com-
22 munications Act of 1934 (47 U.S.C.
23 201–231) as currently enacted or sub-
24 sequently amended; or

1 (III) is an organization not orga-
2 nized to carry on business for their
3 own profit or that of their members;
4 and

5 (ii) includes any entity or person that
6 controls, is controlled by, or is under com-
7 mon control with another covered entity.

8 (B) EXCLUSIONS.—The term “covered en-
9 tity” does not include—

10 (i) a governmental entity such as a
11 body, authority, board, bureau, commis-
12 sion, district, agency, or political subdivi-
13 sion of the Federal, State, or local govern-
14 ment; or

15 (ii) a person or an entity that is col-
16 lecting, processing, or transferring covered
17 data on behalf of or a Federal, State, Trib-
18 al, territorial, or local government entity.

19 (10) DE-IDENTIFIED DATA.—The term “de-
20 identified data” means information that does not
21 identify and is not linked or reasonably linkable to
22 an individual or an individual’s device, regardless of
23 whether the information is aggregated, provided that
24 the covered entity—

1 (A) takes reasonable technical, administra-
2 tive, and physical measures to ensure that the
3 information cannot, at any point, be used to re-
4 identify any individual or device;

5 (B) publicly commits in a clear and con-
6 spicuous manner—

7 (i) to process and transfer the infor-
8 mation solely in a de-identified form with-
9 out any reasonable means for re-identifica-
10 tion; and

11 (ii) to not attempt to re-identify the
12 information with any individual or device;
13 and

14 (C) contractually obligates any person or
15 entity that receives the information from the
16 covered entity to comply with all of the provi-
17 sions of this paragraph.

18 (11) DERIVED DATA.—The term “derived data”
19 means covered data that is created by the derivation
20 of information, data, assumptions, correlations, in-
21 ferences, predictions, or conclusions from facts, evi-
22 dence, or another source of information or data
23 about an individual or an individual’s device.

24 (12) DEVICE.—The term “device” means any
25 electronic equipment capable of transmitting or re-

1 ceiving covered data that is designed for use by one
2 or more individuals.

3 (13) EMPLOYEE.—The term “employee” means
4 (regardless of whether such employee is paid, un-
5 paid, or employed on a temporary basis) an em-
6 ployee, director, officer, staff member, an individual
7 working as a contractor, trainee, volunteer, or intern
8 of an employer.

9 (14) EXECUTIVE AGENCY.—The “Executive
10 agency” has the meaning set forth in section 105 of
11 title 5, United States Code.

12 (15) GENETIC INFORMATION.—The term “ge-
13 netic information” means any covered data, regard-
14 less of its format, that concerns an individual’s ge-
15 netic characteristics, including—

16 (A) raw sequence data that results from
17 the sequencing of an individual’s complete ex-
18 tracted or a portion of the extracted
19 deoxyribonucleic acid (DNA); or

20 (B) genotypic and phenotypic information
21 that results from analyzing the raw sequence
22 data.

23 (16) INDIVIDUAL.—The term “individual”
24 means a natural person residing in the United
25 States.

1 (17) LARGE DATA HOLDER.—The term “large
2 data holder” means a covered entity or service pro-
3 vider that, in the most recent calendar year—

4 (A) had annual gross revenues of
5 \$250,000,000 or more; and

6 (B) collected, processed, or transferred—

7 (i) the covered data of more than
8 5,000,000 individuals or devices that iden-
9 tify or are linked or reasonably linkable to
10 1 or more individuals; and

11 (ii) the sensitive covered data of more
12 than 200,000 individuals or devices that
13 identify or are linked or reasonably
14 linkable to 1 or more individuals.

15 (C) EXCLUSIONS.—The term “large data
16 holder” does not include any instance where the
17 covered entity or service provider would qualify
18 as a large data holder solely on account of col-
19 lecting, or processing—

20 (i) personal email addresses;

21 (ii) personal telephone numbers; or

22 (iii) log-in information of an indi-
23 vidual or device to allow the individual or
24 device to log in to an account administered
25 by the covered entity or service provider.

1 (D) REVENUE.—For purposes of this de-
2 termining whether any covered entity or service
3 provider is a large data holder, the term “rev-
4 enue” as it relates to any covered entity or
5 service provider that is not organized to carry
6 on business for its own profit or that of its
7 members, means the gross receipts the covered
8 entity or service provider received in whatever
9 form from all sources without subtracting any
10 costs or expenses, and includes contributions,
11 gifts, grants, dues or other assessments, income
12 from investments, or proceeds from the sale of
13 real or personal property.

14 (18) MARKET RESEARCH.—The term “market
15 research” means the collection, processing, or trans-
16 fer of covered data as reasonably necessary and pro-
17 portionate to investigate the market for or mar-
18 keting of products, services, or ideas, where the cov-
19 ered data is not—

20 (A) integrated into any product or service;

21 (B) otherwise used to contact any indi-
22 vidual or individual’s device; or

23 (C) used to advertise or market to any in-
24 dividual or individual’s device.

1 (19) MATERIAL.—The term “material” means
2 with respect to an act, practice, or representation of
3 a covered entity (including a representation made by
4 the covered entity in a privacy policy or similar dis-
5 closure to individuals), involving the collection, proc-
6 essing, or transfer of covered data that such act,
7 practice, or representation is likely to affect an indi-
8 vidual’s decision or conduct regarding a product or
9 service.

10 (20) PRECISE GEOLOCATION INFORMATION.—

11 (A) IN GENERAL.—The term “precise
12 geolocation information” means information
13 that reveals the past or present physical loca-
14 tion of an individual, or device that identifies or
15 is linked or reasonably linkable to 1 or more in-
16 dividuals, with sufficient precision to identify
17 street level location information or an individ-
18 ual’s location within a range of 1,000 feet or
19 less.

20 (B) EXCLUSION.—The term “precise
21 geolocation information” does not mean
22 geolocation information identifiable solely from
23 the visual content of an image.

24 (21) PROCESS.—The term “process” means to
25 conduct or direct any operation or set of operations

1 performed on covered data including analyzing, or-
2 ganizing, structuring, retaining, storing, using, or
3 otherwise handling covered data.

4 (22) PROCESSING PURPOSE.—The term “proc-
5 essing purpose” means a reason for which a covered
6 entity collects, processes, or transfers covered data
7 that is specific and granular enough for a reasonable
8 individual to understand the material facts of how
9 and why the covered entity collects, processes, or
10 transfers the covered data.

11 (23) PUBLICLY AVAILABLE INFORMATION.—

12 (A) IN GENERAL.—The term “publicly
13 available information” means any information
14 that a covered entity has a reasonable basis to
15 believe has been lawfully made available to the
16 general public from—

- 17 (i) Federal, State, or local government
18 records provided that the covered entity
19 collects, processes, and transfers such in-
20 formation in accordance with any restric-
21 tions or terms of use placed on the infor-
22 mation by the relevant government entity;
- 23 (ii) widely distributed media;
- 24 (iii) a website or online service made
25 available to all members of the public, for

1 free or for a fee, including where all mem-
2 bers of the public can log-in to the website
3 or online service;

4 (iv) a disclosure that has been made
5 to the general public as required by Fed-
6 eral, State, or local law; or

7 (v) a visual observation of an individ-
8 ual's physical presence in a public place by
9 another person, not including data col-
10 lected by a device in the individual's pos-
11 session.

12 (B) CLARIFICATIONS; LIMITATIONS.—

13 (i) AVAILABLE TO ALL MEMBERS OF
14 THE PUBLIC.—For purposes of this para-
15 graph, information from a website or on-
16 line service is not available to all members
17 of the public if the individual who made
18 the information available via the website or
19 online service has restricted the informa-
20 tion to a specific audience.

21 (ii) OTHER LIMITATIONS.—The term
22 “publicly available information” does not
23 include—

1 (I) any obscene visual depiction
2 (as defined for purposes of section
3 1460 of title 18, United States Code);

4 (II) inferences made exclusively
5 from multiple independent sources of
6 publicly available information that do
7 not reveal sensitive covered data with
8 respect to an individual;

9 (III) biometric information;

10 (IV) publicly available informa-
11 tion that has been combined with cov-
12 ered data;

13 (V) genetic information; or

14 (VI) known nonconsensual inti-
15 mate images.

16 (24) SENSITIVE COVERED DATA.—

17 (A) IN GENERAL.—The term “sensitive
18 covered data” means the following forms of cov-
19 ered data:

20 (i) A government-issued identifier,
21 such as a social security number, passport
22 number, or driver’s license number, that is
23 not required by law to be displayed in pub-
24 lic.

1 (ii) Any information that describes or
2 reveals the past, present, or future physical
3 health, mental health, disability, diagnosis,
4 or healthcare condition or treatment of an
5 individual.

6 (iii) A financial account number, debit
7 card number, credit card number, or infor-
8 mation about income level or bank account
9 balances.

10 (iv) Biometric information.

11 (v) Genetic information.

12 (vi) Precise geolocation information.

13 (vii) An individual's private commu-
14 nications such as voicemails, emails, texts,
15 direct messages, or mail, or information
16 identifying the parties to such communica-
17 tions, voice communications, and any infor-
18 mation that pertains to the transmission of
19 such communications, including telephone
20 numbers called, telephone numbers from
21 which calls were placed, the time calls were
22 made, call duration, and location informa-
23 tion of the parties to the call, unless the
24 covered entity is the sender or an intended
25 recipient of the communication. Commu-

1 communications are not private for purposes of
2 this paragraph if such communications are
3 made from or to a device provided by an
4 employer to an employee insofar as such
5 employer provides conspicuous notice that
6 it may access such communications.

7 (viii) Account or device log-in creden-
8 tials, or security or access codes for an ac-
9 count or device.

10 (ix) Information identifying the sexual
11 orientation or sexual behavior of an indi-
12 vidual in a manner inconsistent with the
13 individual's reasonable expectation regard-
14 ing disclosure of such information.

15 (x) Calendar information, address
16 book information, phone or text logs,
17 photos, audio recordings, or videos main-
18 tained for private use by an individual, re-
19 gardless of whether such information is
20 stored on the individual's device or in a
21 separate location on an individual's device,
22 regardless of whether such information is
23 backed up in a separate location.

24 (xi) A photograph, film, video record-
25 ing, or other similar medium that shows

1 the naked or undergarment-clad private
2 area of an individual.

3 (xii) Information that reveals the
4 video content or services requested or se-
5 lected by an individual from a provider of
6 broadcast television service, cable service,
7 satellite service or streaming media service.

8 (xiii) Information about an individual
9 when the covered entity knows that the in-
10 dividual is under the age of 17.

11 (xiv) Any other covered data collected,
12 processed, or transferred for the purpose
13 of identifying the above data types.

14 (B) RULEMAKING.—The Commission may
15 commence a rulemaking pursuant to section
16 553 of title 5, United States Code, to include
17 any additional category of covered data under
18 this definition that may require a similar level
19 of protection as the data listed in clauses (i)
20 through (xvi) of subparagraph (A) as a result
21 of any new method of collecting, processing, or
22 transferring covered data.

23 (25) SERVICE PROVIDER.—The term “service
24 provider” means a person or entity that collects,
25 processes, or transfers covered data on behalf of,

1 and at the direction of, a covered entity and which
 2 receives covered data from or on behalf of a covered
 3 entity pursuant to a written contract, provided that
 4 the contract meets the requirements of section 302.

5 (26) SERVICE PROVIDER DATA.—The term
 6 “service provider data” means covered data that is
 7 collected or processed by or has been transferred to
 8 a service provider by a covered entity for the pur-
 9 pose of allowing the service provider to perform a
 10 service or function on behalf of, and at the direction
 11 of, such covered entity.

12 (27) STATE.—The term “State” means any of
 13 the 50 States, the District of Columbia, the Com-
 14 monwealth of Puerto Rico, the Virgin Islands,
 15 Guam, American Samoa, the Northern Mariana Is-
 16 lands, or the Trust Territory of the Pacific Islands.

17 (28) STATE PRIVACY AUTHORITY.—

18 (A) IN GENERAL.—The term “State Pri-
 19 vacy Authority” means—

20 (i) the chief consumer protection offi-
 21 cer of a State; or

22 (ii) a State consumer protection agen-
 23 cy with expertise in data protection.

24 (29) SUBSTANTIAL PRIVACY RISK.—The term
 25 “substantial privacy risk” means the collection,

1 processing, or transfer of covered data in a manner
2 that may result in any reasonably foreseeable mate-
3 rial physical injury, economic injury, highly offensive
4 intrusion into the reasonable privacy expectations of
5 an individual under the circumstances, or discrimi-
6 nation on the basis of race, color, religion, national
7 origin, sex, or disability.

8 (30) TARGETED ADVERTISING.—The term “tar-
9 geted advertising”—

10 (A) means displaying to an individual or
11 device identified by a unique identifier an online
12 advertisement or content that is selected based
13 on known or predicted preferences, characteris-
14 tics, or interests associated with the individual
15 or a device identified by a unique identifier; and

16 (B) does not include—

17 (i) advertising or marketing to an in-
18 dividual or an individual’s device in re-
19 sponse to the individual’s specific request
20 for information or feedback;

21 (ii) contextual advertising, which is
22 when an advertisement is displayed based
23 on the content or location in which the ad-
24 vertisement appears and does not vary

1 based on who is viewing the advertisement;
2 or

3 (iii) processing covered data solely for
4 measuring or reporting advertising or con-
5 tent, performance, reach, or frequency, in-
6 cluding independent measurement.

7 (31) THIRD PARTY.—The term “third party”—

8 (A) means any person or entity that—

9 (i) collects, processes, or transfers
10 third-party data; and

11 (ii) is not a service provider with re-
12 spect to such data; and

13 (B) does not include a person or entity
14 that collects covered data from another entity if
15 the 2 entities are related by common ownership
16 or corporate control and share common brand-
17 ing, unless one of those is a large data holder
18 or those entities are each related to a large data
19 holder through common ownership or corporate
20 control.

21 (32) THIRD-PARTY COLLECTING ENTITY.—

22 (A) IN GENERAL.—The term “third-party
23 collecting entity”—

24 (i) means a covered entity whose prin-
25 cipal source of revenue is derived from

1 processing or transferring the covered data
2 that the covered entity did not collect di-
3 rectly from the individuals linked or
4 linkable to the covered data; and

5 (ii) does not include a covered entity
6 in so far as such entity processes employee
7 data collected by and received from a third
8 party concerning any individual who is an
9 employee of the third party for the sole
10 purpose of such third party providing ben-
11 efits to the employee.

12 (B) PRINCIPAL SOURCE OF REVENUE DE-
13 FINED.—For purposes of this paragraph, “prin-
14 cipal source of revenue” means, for the prior
15 12-month period, either—

16 (i) more than 50 percent of all rev-
17 enue of the covered entity; or

18 (ii) obtaining revenue from processing
19 or transferring the covered data of more
20 than 5,000,000 individuals that the cov-
21 ered entity did not collect directly from the
22 individuals to which the covered data per-
23 tains.

24 (C) NON-APPLICATION TO SERVICE PRO-
25 VIDERS.—An entity shall not be considered to

1 be a third-party collecting entity for purposes of
2 this Act if the entity is acting as a service pro-
3 vider (as defined in this section).

4 (33) THIRD-PARTY DATA.—The term “third-
5 party data” means covered data that has been trans-
6 ferred to a third party by a covered entity.

7 (34) TRANSFER.—The term “transfer” means
8 to disclose, release, share, disseminate, make avail-
9 able, or license in writing, electronically, or by any
10 other means.

11 (35) UNIQUE IDENTIFIER.—The term “unique
12 identifier” means an identifier to the extent that
13 such identifier is reasonably linkable to an individual
14 or device that identifies or is linked or reasonably
15 linkable to 1 or more individuals, including a device
16 identifier, an Internet Protocol address, cookies, bea-
17 cons, pixel tags, mobile ad identifiers, or similar
18 technology, customer number, unique pseudonym, or
19 user alias, telephone numbers, or other forms of per-
20 sistent or probabilistic identifiers that are linked or
21 reasonably linkable to an individual or device.

22 (36) WIDELY DISTRIBUTED MEDIA.—The term
23 “widely distributed media” means information that
24 is available to the general public, including informa-
25 tion from a telephone book or online directory, a tel-

1 evision, internet, or radio program, the news media,
 2 or an internet site that is available to the general
 3 public on an unrestricted basis, but does not include
 4 an obscene visual depiction (as defined in section
 5 1460 of title 18, United States Code).

6 **TITLE I—DUTY OF LOYALTY**

7 **SEC. 101. DATA MINIMIZATION.**

8 (a) IN GENERAL.—A covered entity shall not collect,
 9 process, or transfer covered data unless the collection,
 10 processing, or transfer is limited to what is reasonably
 11 necessary and proportionate to—

12 (1) provide, or maintain a specific product or
 13 service requested by the individual to whom the data
 14 pertains;

15 (2) deliver a communication that is reasonably
 16 anticipated by the individual recipient within the
 17 context of the individual’s interactions with the cov-
 18 ered entity; or

19 (3) effect a purpose expressly permitted under
 20 subsection (b).

21 (b) PERMISSIBLE PURPOSES.—A covered entity or
 22 service provider may collect, process, or transfer covered
 23 data for any of the following purposes provided that the
 24 covered entity or service provider can demonstrate that
 25 collection, processing, or transfer complies with all other

1 applicable laws not preempted in section 404 and provi-
2 sions of this Act and is limited to what is reasonably nec-
3 essary and proportionate to such purpose:

4 (1) To initiate or complete a transaction or ful-
5 fill an order or service specifically requested by an
6 individual, including any associated routine adminis-
7 trative activity such as billing, shipping, delivery,
8 and accounting, including the collection, processing,
9 or transferring of the last four digits of a credit card
10 number.

11 (2) With respect to covered data previously col-
12 lected in accordance with this Act, notwithstanding
13 this exception, to process such data as necessary to
14 perform system maintenance or diagnostics, to main-
15 tain a product or service for which such data was
16 collected, to conduct internal research or analytics,
17 to improve a product or service for which such data
18 was collected and to perform inventory management
19 or reasonable network management, to protect
20 against spam, or to debug or repair errors that im-
21 pair the functionality of a service or product for
22 which such data was collected.

23 (3) To authenticate users of a product or serv-
24 ice.

1 (4) To prevent, detect, protect against, or re-
2 spond to a security incident, or fulfill a product or
3 service warranty. For purposes of this paragraph,
4 security is defined as network security as well as in-
5 trusion, medical alerts, fire alarms, and access con-
6 trol security.

7 (5) To prevent, detect, protect against or re-
8 spond to fraud, harassment, or illegal activity. For
9 the purposes of this paragraph, illegal activity means
10 a violation of a Federal, State, or local law punish-
11 able as a felony or misdemeanor that can directly
12 harm another person.

13 (6) To comply with a legal obligation imposed
14 by Federal, Tribal, Local, or State law, or to estab-
15 lish, exercise, or defend legal claims.

16 (7) To prevent an individual, or groups of indi-
17 viduals, from suffering harm where the covered enti-
18 ty or service provider believes in good faith that the
19 individual, or groups of individuals, is at risk of
20 death, serious physical injury, or other serious
21 health risk.

22 (8) To effectuate a product recall pursuant to
23 Federal or State law.

1 (9)(A) To conduct a public or peer-reviewed sci-
2 entific, historical, or statistical research project
3 that—

4 (i) is in the public interest;

5 (ii) adheres to all relevant laws governing
6 such research; and

7 (iii) adheres to the regulations for human
8 subject research established under part 46 of
9 title 45, Code of Federal Regulations (or a suc-
10 cessor regulations).

11 (B) The Commission should set forth within 18
12 months of the enactment of this Act guidelines to
13 help covered entities ensure the privacy of affected
14 users and the security of covered data, particularly
15 as data is being transferred to and stored by re-
16 searchers.

17 (10) To deliver a communication at the direc-
18 tion of an individual between the communicating in-
19 dividual and one or more individuals or entities.

20 (11) With respect to covered data previously
21 collected in accordance with this Act, notwith-
22 standing this exception, to process such data as nec-
23 essary to provide first party marketing or adver-
24 tising of products or services provided by the covered
25 entity.

1 (12) Otherwise complies with the requirements
2 of this Act, including section 204(c), to provide a
3 targeted advertisement.

4 (c) GUIDANCE.—The Commission shall issue guid-
5 ance regarding what is reasonably necessary and propor-
6 tionate to comply with this section. Such guidance shall
7 take into consideration—

8 (1) the size of, and the nature, scope, and com-
9 plexity of the activities engaged in by the covered en-
10 tity, including whether the covered entity is a large
11 data holder, nonprofit organization, covered entities
12 meeting the requirements of section 209, service pro-
13 vider, third party, or third-party collecting entity;

14 (2) the sensitivity of covered data collected,
15 processed, or transferred by the covered entity;

16 (3) the volume of covered data collected, proc-
17 essed, or transferred by the covered entity; and

18 (4) the number of individuals and devices to
19 which the covered data collected, processed, or trans-
20 ferred by the covered entity relates.

21 (d) DECEPTIVE MARKETING OF A PRODUCT OR
22 SERVICE.—A covered entity, service provider, or third
23 party is prohibited from engaging in deceptive advertising
24 or marketing with respect to a product or service provided
25 to an individual.

1 **SEC. 102. LOYALTY DUTIES.**

2 (a) RESTRICTED DATA PRACTICES.—Notwith-
3 standing section 101 and unless an exception applies, with
4 respect to covered data, a covered entity shall not—

5 (1) collect, process, or transfer a social security
6 number, except when necessary to facilitate exten-
7 sions of credit, authentication, the payment and col-
8 lection of taxes, the enforcement of a contract be-
9 tween parties, or the prevention, investigation, and
10 prosecution of fraud or illegal activity;

11 (2) collect or process sensitive covered data, ex-
12 cept where such collection or processing is strictly
13 necessary to provide or maintain a specific product
14 or service requested by the individual to whom the
15 covered data pertains, or to effect a purpose enu-
16 merated in section 101(b)(1) through (10);

17 (3) transfer an individual's sensitive covered
18 data to a third party, unless—

19 (A) the transfer is made pursuant to the
20 affirmative express consent of the individual;

21 (B) the transfer is necessary to comply
22 with a legal obligation imposed by Federal,
23 State, or local law, or to establish, exercise, or
24 defend legal claims;

25 (C) the transfer is necessary to prevent an
26 individual from imminent injury where the cov-

1 ered entity believes in good faith that the indi-
2 vidual is at risk of death or serious physical in-
3 jury;

4 (D) the transfer of biometric information
5 is necessary to facilitate data security or au-
6 thentication;

7 (E) the transfer of a password is necessary
8 to use a designated password manager or is to
9 a covered entity for the exclusive purpose of
10 identifying passwords that are being re-used
11 across sites or accounts; or

12 (F) the transfer of genetic information is
13 necessary to perform a medical diagnosis or
14 medical treatment specifically requested by an
15 individual, or to conduct medical research in ac-
16 cordance with conditions of section 101(b)(9);
17 or

18 (4) collect, process, or transfer an individual's
19 aggregated internet search or browsing history, ex-
20 cept with the affirmative express consent of the indi-
21 vidual or pursuant to one of the permissible pur-
22 poses enumerated in section 101(b)(1) through (10).

23 **SEC. 103. PRIVACY BY DESIGN.**

24 (a) **POLICIES, PRACTICES, AND PROCEDURES.**—A
25 covered entity and a service provider shall establish, imple-

1 ment, and maintain reasonable policies, practices, and pro-
2 cedures regarding the collection, processing, and transfer
3 of covered data to—

4 (1) consider Federal laws, rules, or regulations
5 related to covered data the covered entity or service
6 provider collects, processes, or transfers;

7 (2) identify, assess, and mitigate privacy risks
8 related to individuals under the age of 17, if applica-
9 ble;

10 (3) mitigate privacy risks, including substantial
11 privacy risks, related to the products and services of
12 the covered entity or the service provider, including
13 their design, development, and implementation; and

14 (4) implement reasonable training and safe-
15 guards within the covered entity and service provider
16 to promote compliance with all privacy laws applica-
17 ble to covered data the covered entity collects, proc-
18 esses, or transfers or covered data the service pro-
19 vider collects, processes, or transfers on behalf of the
20 covered entity and mitigate privacy risks, including
21 substantial privacy risks.

22 (b) FACTORS TO CONSIDER.—The policies, practices,
23 and procedures established by a covered entity and a serv-
24 ice provider under subsection (a), shall correspond with—

1 (1) the size of the covered entity or the service
2 provider and the nature, scope, and complexity of
3 the activities engaged in by the covered entity, in-
4 cluding whether the covered entity is a large data
5 holder, nonprofit organization, covered entities meet-
6 ing the requirements of section 209, third party, or
7 third-party collecting entity;

8 (2) the sensitivity of the covered data collected,
9 processed, or transferred by the covered entity or
10 service provider;

11 (3) the volume of covered data collected, proc-
12 essed, or transferred by the covered entity or service
13 provider;

14 (4) the number of individuals and devices to
15 which the covered data collected, processed, or trans-
16 ferred by the covered entity or service provider re-
17 lates; and

18 (5) the cost of implementing such policies, prac-
19 tices, and procedures in relation to the risks and na-
20 ture of the covered data.

21 (c) COMMISSION GUIDANCE.—Not later than 1 year
22 after the date of enactment of this Act, the Commission
23 shall issue guidance as to what constitutes reasonable poli-
24 cies, practices, and procedures as required by this section.
25 The Commission shall consider unique circumstances ap-

1 plicable to nonprofit organizations and covered entities
2 meeting the requirements of section 209.

3 **SEC. 104. LOYALTY TO INDIVIDUALS WITH RESPECT TO**
4 **PRICING.**

5 (a) **CONDITIONAL SERVICE OR PRICING PROHIB-**
6 **ITED.**—A covered entity shall not deny or condition or ef-
7 fectively condition the provision of a service or product to
8 an individual based on the individual’s agreement to waive
9 (or refusal to waive) any requirements under this Act or
10 any regulations promulgated under this Act or terminate
11 a service or otherwise refuse to provide a service or prod-
12 uct to an individual as a consequence of the individual’s
13 refusal to provide such a waiver.

14 (b) **RULES OF CONSTRUCTION.**—Nothing in sub-
15 section (a) shall be construed to—

16 (1) prohibit the relation of the price of a service
17 or the level of service provided to an individual to
18 the provision, by the individual, of financial informa-
19 tion that is necessarily collected and processed only
20 for the purpose of initiating, rendering, billing for,
21 or collecting payment for a service or product re-
22 quested by the individual;

23 (2) prohibit a covered entity from offering a
24 loyalty program that provides discounted or free
25 products or services, or other consideration, in ex-

change for an individual's continued business with the covered entity, provided that such program otherwise complies with the requirements of this Act and any regulations promulgated under this Act;

(3) require a covered entity to provide a loyalty program that would require the covered entity to collect, process, or transfer covered data that it otherwise would not;

(4) prohibit a covered entity from offering a financial incentive or other consideration to an individual for participation in market research; or

(5) prohibit a covered entity from offering different types of pricing or functionalities with respect to a product or service based on an individual's exercise of a right in section 203(a)(3).

TITLE II—CONSUMER DATA RIGHTS

SEC. 201. CONSUMER AWARENESS.

(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Commission shall publish, on the public website of the Commission, a web page that describes each provision, right, obligation, and requirement of this Act, listed separately for individuals and for covered entities and service providers, and the remedies, exemptions, and protections associated with this Act

1 in plain and concise language and in an easy-to-under-
2 stand manner.

3 (b) UPDATES.—The Commission shall update the in-
4 formation published under subsection (a) on a quarterly
5 basis as necessitated by any change in law, regulation,
6 guidance, or judicial decisions.

7 (c) ACCESSIBILITY.—The Commission shall publish
8 materials disclosed pursuant to subsection (a) in the ten
9 languages with the most users in the United States, ac-
10 cording to the most recent U.S. Census. The Commission
11 shall ensure the website is readily accessible to and usable
12 by individuals with disabilities.

13 **SEC. 202. TRANSPARENCY.**

14 (a) IN GENERAL.—Each covered entity and service
15 provider shall make publicly available, in a clear, con-
16 spicuous, not misleading, and readily accessible manner,
17 a privacy policy that provides a detailed and accurate rep-
18 resentation of the entity’s data collection, processing, and
19 transfer activities.

20 (b) CONTENT OF PRIVACY POLICY.—The privacy pol-
21 icy required under subsection (a) shall include, at a min-
22 imum, the following:

23 (1) The identity and the contact information
24 of—

1 (A) the covered entity or service provider
2 (including the covered entity's or service pro-
3 vider's points of contact, generic electronic mail
4 addresses, and phone numbers of the covered
5 entity, as applicable for privacy and data secu-
6 rity inquiries); and

7 (B) any other entity within the same cor-
8 porate structure as, and under common brand-
9 ing with, the covered entity or service provider
10 to which covered data is transferred by the cov-
11 ered entity.

12 (2) The categories of covered data the covered
13 entity or service provider collects or processes.

14 (3) The processing purposes for each category
15 of covered data the covered entity or service provider
16 collects or processes.

17 (4) Whether the covered entity or service pro-
18 vider transfers covered data and, if so, each category
19 of service provider and third party to which the cov-
20 ered entity or service provider transfers covered
21 data, the name of each third-party collecting entity
22 to which the covered entity or service provider trans-
23 fers covered data, and the purposes for which such
24 data is transferred to such categories of service pro-
25 viders and third parties or third-party collecting en-

1 tities, except for transfers to governmental entities
2 pursuant to a court order or law that prohibits the
3 covered entity from disclosing such transfer.

4 (5) The length of time the covered entity or
5 service provider intends to retain each category of
6 covered data, including sensitive covered data, or, if
7 it is not possible to identify that time frame, the cri-
8 teria used to determine the length of time the cov-
9 ered entity intends to retain categories of covered
10 data.

11 (6) A prominent description of how an indi-
12 vidual can exercise the rights described in this Act.

13 (7) A general description of the covered entity's
14 or service provider's data security practices.

15 (8) The effective date of the privacy policy.

16 (9) Whether or not any covered data collected
17 by the covered entity or service provider is trans-
18 ferred to, processed in, stored in or otherwise acces-
19 sible to the People's Republic of China, Russia, Iran,
20 or North Korea.

21 (c) LANGUAGES.—The privacy policy required under
22 subsection (a) shall be made available to the public in each
23 language in which the covered entity or service provider—

24 (1) provides a product or service that is subject
25 to the privacy policy; or

1 (2) carries out activities related to such product
2 or service.

3 (d) ACCESSIBILITY.—The covered entity or service
4 provider shall also provide the disclosures under this sec-
5 tion in a manner that is readily accessible to and usable
6 by individuals with disabilities.

7 (e) MATERIAL CHANGES.—

8 (1) AFFIRMATIVE EXPRESS CONSENT.—If a
9 covered entity makes a material change to its pri-
10 vacy policy or practices, the covered entity shall no-
11 tify each individual affected by such material change
12 before implementing the material change with re-
13 spect to any previously collected covered data and,
14 except as provided in section 101(b), provide a rea-
15 sonable opportunity for each individual to withdraw
16 consent to any further materially different collection,
17 processing, or transferring of covered data under the
18 changed policy.

19 (2) NOTIFICATION.—The covered entity shall
20 take all reasonable measures to provide direct notifi-
21 cation regarding material changes to the privacy pol-
22 icy to each affected individual, in each language that
23 the privacy policy is made available, and taking into
24 account available technology and the nature of the
25 relationship.

1 (3) CLARIFICATION.—Nothing in this section
2 shall be construed to affect the requirements for cov-
3 ered entities under section 102 or 204.

4 (4) LOG OF MATERIAL CHANGES.—Each large
5 data holder shall retain copies of previous versions
6 of its privacy policy for at least 10 years and publish
7 them on its website. It shall make publicly available,
8 in a clear, conspicuous, and readily accessible man-
9 ner, a log describing the data and nature of each
10 material change over the past 10 years. The descrip-
11 tions shall be sufficient for a reasonable individual
12 to understand the material effect of each material
13 change.

14 (f) SHORT-FORM NOTICE TO CONSUMERS BY LARGE
15 DATA HOLDERS.—

16 (1) IN GENERAL.—In addition to the privacy
17 policy required under subsection (a), a large data
18 holder must provide a short-form notice of its cov-
19 ered data practices in a manner that is—

20 (A) concise, clear, and conspicuous;

21 (B) readily accessible, based on the way an
22 individual interacts with the large data holder
23 and its products or services and what is reason-
24 ably anticipated within the context of the rela-
25 tionship;

1 (C) inclusive of an overview of individual
2 rights and disclosures to reasonably draw atten-
3 tion to data practices that may reasonably be
4 unexpected or that involve sensitive covered
5 data; and

6 (D) no more than 500 words in length.

7 (2) RULEMAKING.—The Commission shall issue
8 a rule pursuant to section 553 of title 5, United
9 States Code, establishing the minimum data disclo-
10 sures necessary for the short-form notice which shall
11 not exceed the content requirements in subsection
12 (b) and shall include templates and/or models of
13 short-form notices.

14 **SEC. 203. INDIVIDUAL DATA OWNERSHIP AND CONTROL.**

15 (a) ACCESS TO, AND CORRECTION, DELETION, AND
16 PORTABILITY OF, COVERED DATA.—Subject to sub-
17 sections (b) and (c), a covered entity shall provide an indi-
18 vidual, after receiving a verified request from the indi-
19 vidual, with the right to—

20 (1) access—

21 (A) the covered data, except covered data
22 in back-up or archival systems, of the individual
23 in a human-readable format that a reasonable
24 individual can understand and download from
25 the internet, that is collected, processed, or

1 transferred by the covered entity or any service
2 provider of the covered entity within the 24
3 months preceding the request;

4 (B) the name of any third party and the
5 categories of any service providers to whom the
6 covered entity has transferred for consideration
7 the covered data of the individual, as well as
8 the categories of sources from which the cov-
9 ered data was collected; and

10 (C) a description of the purpose for which
11 the covered entity transferred the covered data
12 of the individual to a third party or service pro-
13 vider;

14 (2) correct any verifiably material inaccuracy or
15 materially incomplete information with respect to the
16 covered data of the individual that is processed by
17 the covered entity and instruct the covered entity to
18 notify any third party, or service provider to which
19 the covered entity transferred such covered data of
20 the corrected information;

21 (3) delete covered data of the individual that is
22 processed by the covered entity and instruct the cov-
23 ered entity to notify any third party, or service pro-
24 vider to which the covered entity transferred such
25 covered data of the individual's deletion request; and

1 (4) to the extent technically feasible, export cov-
2 ered data to the individual or directly to another en-
3 tity, except for derived data, of the individual that
4 is processed by the covered entity without licensing
5 restrictions that limit such transfers, in—

6 (A) a human-readable format that a rea-
7 sonable individual can understand and
8 download from the internet; and

9 (B) a portable, structured, interoperable,
10 and machine-readable format.

11 (b) INDIVIDUAL AUTONOMY.—A covered entity shall
12 not condition, effectively condition, attempt to condition,
13 or attempt to effectively condition the exercise of any indi-
14 vidual rights under this section through—

15 (1) through the use of any false, fictitious,
16 fraudulent, or materially misleading statement or
17 representation; or

18 (2) the design, modification, or manipulation of
19 any user interface with the purpose or substantial
20 effect of obscuring, subverting, or impairing a rea-
21 sonable individual's autonomy, decision making, or
22 choice to exercise any such rights.

23 (c) TIMING.—

24 (1) Subject to subsections (d) and (e)(1) each
25 request shall be completed by any—

1 (A) large data holder within 45 days of
2 verification of such request from an individual;

3 (B) covered entity that is not considered a
4 large data holder or a covered entity described
5 in section 209 within 60 days of verification of
6 such request from an individual; or

7 (C) covered entity as described in section
8 209 within 90 days of verification of such re-
9 quest from an individual.

10 (2) A response period set forth in this sub-
11 section may be extended once by 45 additional days
12 when reasonably necessary, considering the com-
13 plexity and number of the individual's requests, so
14 long as the covered entity informs the individual of
15 any such extension within the initial 45-day response
16 period, together with the reason for the extension.

17 (d) FREQUENCY AND COST OF ACCESS.—A covered
18 entity—

19 (1) shall provide an individual with the oppor-
20 tunity to exercise each of the rights described in
21 subsection (a); and

22 (2) with respect to—

23 (A) the first 2 times that an individual ex-
24 ercises any right described in subsection (a) in

1 any 12-month period, shall allow the individual
2 to exercise such right free of charge; and

3 (B) any time beyond the initial 2 times de-
4 scribed in subparagraph (A), may allow the in-
5 dividual to exercise such right for a reasonable
6 fee for each request.

7 (e) VERIFICATION AND EXCEPTIONS.—

8 (1) REQUIRED EXCEPTIONS.—A covered entity
9 shall not permit an individual to exercise a right de-
10 scribed in subsection (a), in whole or in part, if the
11 covered entity—

12 (A) cannot reasonably verify that the indi-
13 vidual making the request to exercise the right
14 is the individual whose covered data is the sub-
15 ject of the request or an individual authorized
16 to make such a request on the individual's be-
17 half;

18 (B) reasonably believes that the request is
19 made to interfere with a contract between the
20 covered entity and another individual;

21 (C) determines that the exercise of the
22 right would require access to or correction of
23 another individual's sensitive covered data; or

24 (D) reasonably believes that the exercise of
25 the right would require the covered entity to en-

1 gage in an unfair or deceptive practice under
2 section 5 of the Federal Trade Commission Act
3 (15 U.S.C. 45).

4 (2) ADDITIONAL INFORMATION.—If a covered
5 entity cannot reasonably verify that a request to ex-
6 ercise a right described in subsection (a) is made by
7 the individual whose covered data is the subject of
8 the request (or an individual authorized to make
9 such a request on the individual’s behalf), the cov-
10 ered entity—

11 (A) may request that the individual mak-
12 ing the request to exercise the right provide any
13 additional information necessary for the sole
14 purpose of verifying the identity of the indi-
15 vidual; and

16 (B) shall not process or transfer such addi-
17 tional information for any other purpose.

18 (3) PERMISSIVE EXCEPTIONS.—

19 (A) IN GENERAL.—A covered entity may
20 decline to comply with a request to exercise a
21 right described in subsection (a), in whole or in
22 part, that would—

23 (i) require the covered entity to retain
24 any covered data collected for a single,
25 one-time transaction, if such covered data

1 is not processed or transferred by the cov-
2 ered entity for any purpose other than
3 completing such transaction;

4 (ii) be impossible or demonstrably im-
5 practicable to comply with, and the covered
6 entity shall provide a description to the re-
7 questor detailing the inability to comply
8 with the request;

9 (iii) require the covered entity to at-
10 tempt to re-identify de-identified data;

11 (iv) result in the release of trade se-
12 crets, or other privileged, or confidential
13 business information;

14 (v) require the covered entity to cor-
15 rect any covered data that cannot be rea-
16 sonably verified as being inaccurate or in-
17 complete;

18 (vi) interfere with law enforcement,
19 judicial proceedings, investigations, or rea-
20 sonable efforts to guard against, detect, or
21 investigate malicious or unlawful activity,
22 or enforce valid contracts;

23 (vii) violate Federal or State law or
24 the rights and freedoms of another indi-

vidual, including under the Constitution of the United States;

(viii) prevent a covered entity from being able to maintain a confidential record of deletion requests, maintained solely for the purpose of preventing covered data of an individual who has submitted a deletion request and requests that the covered entity no longer collect, process, or transfer such data;

(ix) fall within an exception enumerated in the regulations promulgated by the Commission pursuant to paragraph (D); or

(x) with respect to requests for deletion—

(I) unreasonably interfere with the provision of products or services by the covered entity to another person it currently serves;

(II) delete covered data that relates to a public figure and for which the requesting individual has no reasonable expectation of privacy;

(III) delete covered data reasonably necessary to perform a contract

1 between the covered entity and the in-
2 dividual;

3 (IV) delete covered data that the
4 covered entity needs to retain in order
5 to comply with professional ethical ob-
6 ligations; or

7 (V) delete covered data that the
8 covered entity reasonably believes may
9 be evidence of unlawful activity or an
10 abuse of the covered entity's products
11 or services.

12 (B) PARTIAL COMPLIANCE.—In a cir-
13 cumstance that would allow a denial pursuant
14 to paragraph (A), a covered entity shall par-
15 tially comply with the remainder of the request
16 if it is possible and not unduly burdensome to
17 do so.

18 (C) NUMBER OF REQUESTS.—For pur-
19 poses of this paragraph, the receipt of a large
20 number of verified requests, on its own, shall
21 not be considered to render compliance with a
22 request demonstrably impossible.

23 (D) FURTHER EXCEPTIONS.—The Com-
24 mission may, by regulation as described in sub-
25 section (f), establish additional permissive ex-

1 ceptions necessary to protect the rights of indi-
2 viduals, alleviate undue burdens on covered en-
3 tities, prevent unjust or unreasonable outcomes
4 from the exercise of access, correction, deletion,
5 or portability rights, or as otherwise necessary
6 to fulfill the purposes of this section. In cre-
7 ating such exceptions, the Commission should
8 consider any relevant changes in technology,
9 means for protecting privacy and other rights,
10 and beneficial uses of covered data by covered
11 entities.

12 (f) REGULATIONS.—Within two years of the date of
13 enactment of this Act, the Commission may promulgate
14 regulations, pursuant to section 553 of title 5, United
15 States Code (5 U.S.C. 553), as necessary to establish
16 processes by which covered entities are to comply with the
17 provisions of this section. Such regulations shall take into
18 consideration—

19 (1) the size of, and the nature, scope, and com-
20 plexity of the activities engaged in by the covered en-
21 tity, including whether the covered entity is a large
22 data holder, nonprofit organization, covered entities
23 meeting the requirements of section 209, service pro-
24 vider, third party, or third-party collecting entity;

1 (2) the sensitivity of covered data collected,
2 processed, or transferred by the covered entity;

3 (3) the volume of covered data collected, proc-
4 essed, or transferred by the covered entity; and

5 (4) the number of individuals and devices to
6 which the covered data collected, processed, or trans-
7 ferred by the covered entity relates.

8 (g) ACCESSIBILITY.—A covered entity shall facilitate
9 the ability for individuals to make requests under this sec-
10 tion in any of the ten languages with the most users in
11 the United States, according to the most recent U.S. Cen-
12 sus, if the covered entity provides service in such language.
13 The mechanisms by which a covered entity enables individ-
14 uals to make requests under this section shall be readily
15 accessible and usable by with disabilities.

16 **SEC. 204. RIGHT TO CONSENT AND OBJECT.**

17 (a) WITHDRAWAL OF CONSENT.—A covered entity
18 shall provide an individual with a clear and conspicuous,
19 easy-to-execute means to withdraw any affirmative express
20 consent previously provided by the individual that is as
21 easy to execute by a reasonable individual as the means
22 to provide consent, with respect to the processing or trans-
23 fer of the covered data of the individual.

24 (b) RIGHT TO OPT OUT OF COVERED DATA TRANS-
25 FERS.—

1 (1) IN GENERAL.—A covered entity—

2 (A) shall not transfer the covered data of
3 an individual to a third party if the individual
4 objects to the transfer; and

5 (B) shall allow an individual to object to
6 such transfer through an opt-out mechanism, as
7 described in section 210, if applicable.

8 (2) EXCEPTION.—An individual may not opt
9 out of the collection, processing, and transfer of cov-
10 ered data made pursuant to the exceptions in sec-
11 tions 101(b)(1) through (11) of this Act.

12 (c) RIGHT TO OPT OUT OF TARGETED ADVER-
13 TISING.—A covered entity that engages in targeted adver-
14 tising shall—

15 (1) prior to engaging in such targeted adver-
16 tising and at all times thereafter, provide an indi-
17 vidual with a clear and conspicuous means to opt
18 out of targeted advertising;

19 (2) abide by such opt-out designations by an in-
20 dividual; and

21 (3) allow an individual to prohibit such targeted
22 advertising through an opt-out mechanism, as de-
23 scribed in section 210, if applicable.

24 (d) INDIVIDUAL AUTONOMY.—A covered entity shall
25 not condition, effectively condition, attempt to condition,

1 or attempt to effectively condition the exercise of any indi-
2 vidual rights under this section through—

3 (1) through the use of any false, fictitious,
4 fraudulent, or materially misleading statement or
5 representation; or

6 (2) the design, modification, or manipulation of
7 any user interface with the purpose or substantial
8 effect of obscuring, subverting, or impairing a rea-
9 sonable individual's autonomy, decision making, or
10 choice to exercise any such rights.

11 **SEC. 205. DATA PROTECTIONS FOR CHILDREN AND MI-**
12 **NORS.**

13 (a) PROHIBITION ON TARGETED ADVERTISING TO
14 CHILDREN AND MINORS.—A covered entity shall not en-
15 gage in targeted advertising to any individual under the
16 age of 17 if the covered entity knows that the individual
17 is under the age of 17.

18 (b) DATA TRANSFER REQUIREMENTS RELATED TO
19 MINORS.—A covered entity shall not transfer the covered
20 data of an individual to a third party without affirmative
21 express consent from the individual or the individual's par-
22 ent or guardian if the covered entity knows that the indi-
23 vidual under the age of 17.

24 (c) KNOWLEDGE.—The knowledge requirement in
25 subsections (a) and (b), shall not be construed to require

1 the affirmative collection or processing of any data with
2 respect to the age of an individual or a proxy thereof, or
3 to require that a covered entity implement an age gating
4 regime. Rather, the determination of whether an indi-
5 vidual is under 17 shall be based on the covered data col-
6 lected directly from an individual or a proxy thereof that
7 the covered entity would otherwise collect in the normal
8 course of business.

9 (d) YOUTH PRIVACY AND MARKETING DIVISION.—

10 (1) ESTABLISHMENT.—There is established
11 within the Commission a division to be known as the
12 “Youth Privacy and Marketing Division” (in this
13 section referred to as the “Division”).

14 (2) DIRECTOR.—The Division shall be headed
15 by a Director, who shall be appointed by the Chair
16 of the Commission.

17 (3) DUTIES.—The Division shall be responsible
18 for assisting the Commission in addressing, as it re-
19 lates to this Act—

20 (A) the privacy of children and minors;
21 and

22 (B) marketing directed at children and mi-
23 nors.

24 (4) STAFF.—The Director of the Division shall
25 hire adequate staff to carry out the duties described

1 in paragraph (3), including by hiring individuals who
2 are experts in data protection, digital advertising,
3 data analytics, and youth development.

4 (5) REPORTS.—Not later than 1 year after the
5 date of enactment of this Act, and annually there-
6 after, the Commission shall submit to the Committee
7 on Commerce, Science, and Transportation of the
8 Senate and the Committee on Energy and Com-
9 merce of the House of Representatives a report that
10 includes—

11 (A) a description of the work of the Divi-
12 sion regarding emerging concerns relating to
13 youth privacy and marketing practices; and

14 (B) an assessment of how effectively the
15 Division has, during the period for which the
16 report is submitted, assisting the Commission
17 to address youth privacy and marketing prac-
18 tices.

19 (6) PUBLICATION.—Not later than 10 days
20 after the date on which a report is submitted under
21 paragraph (5), the Commission shall publish the re-
22 port on its website.

23 (e) REPORT BY THE INSPECTOR GENERAL.—

24 (1) IN GENERAL.—Not later than 2 years after
25 the date of enactment of this Act, and biennially

1 thereafter, the Inspector General of the Commission
2 shall submit to the Commission and to the Com-
3 mittee on Commerce, Science, and Transportation of
4 the Senate and the Committee on Energy and Com-
5 merce of the House of Representatives a report re-
6 garding the safe harbor provisions in section 1307 of
7 the Children’s Online Privacy Protection Act of
8 1998 (15 U.S.C. 6503), which shall include—

9 (A) an analysis of whether the safe harbor
10 provisions are—

11 (i) operating fairly and effectively;

12 and

13 (ii) effectively protecting the interests
14 of children and minors; and

15 (B) any proposal or recommendation for
16 policy changes that would improve the effective-
17 ness of the safe harbor provisions.

18 (2) PUBLICATION.—Not later than 10 days
19 after the date on which a report is submitted under
20 paragraph (1), the Commission shall publish the re-
21 port on the website of the Commission.

22 **SEC. 206. THIRD-PARTY COLLECTING ENTITIES.**

23 (a) NOTICE.—Each third-party collecting entity shall
24 place a clear and conspicuous notice on the website or mo-
25 bile application of the third-party collecting entity (if the

1 third-party collecting entity maintains such a website or
2 mobile application) that—

3 (1) notifies individuals that the entity is a
4 third-party collecting entity using specific language
5 that the Commission shall develop through rule-
6 making under section 553 of title 5, United States
7 Code; and

8 (2) includes a link to the website established
9 under subsection (b)(3).

10 (b) THIRD-PARTY COLLECTING ENTITY REGISTRA-
11 TION.—

12 (1) IN GENERAL.—Not later than January 31
13 of each calendar year that follows a calendar year
14 during which a covered entity acted as a third-party
15 collecting entity and processed covered data per-
16 taining to more than 5,000 individuals or devices
17 that identify or are linked or reasonably linkable to
18 an individual, such covered entity shall register with
19 the Commission in accordance with this subsection.

20 (2) REGISTRATION REQUIREMENTS.—In reg-
21 istering with the Commission as required under
22 paragraph (1), a third-party collecting entity shall
23 do the following:

24 (A) Pay to the Commission a registration
25 fee of \$100.

1 (B) Provide the Commission with the fol-
2 lowing information:

3 (i) The legal name and primary phys-
4 ical, email, and internet addresses of the
5 third-party collecting entity.

6 (ii) A description of the categories of
7 data the third-party collecting entity proc-
8 esses and transfers.

9 (iii) The contact information of the
10 third-party collecting entity, including a
11 contact person, telephone number, an e-
12 mail address, a website, and a physical
13 mailing address.

14 (iv) Link to a website through which
15 an individual may easily exercise the rights
16 provided under this subsection.

17 (3) THIRD-PARTY COLLECTING ENTITY REG-
18 ISTRY.—The Commission shall establish and main-
19 tain on a website a searchable, publicly available,
20 central registry of third-party collecting entities that
21 are registered with the Commission under this sub-
22 section that includes the following:

23 (A) A listing of all registered third-party
24 collecting entities and a search feature that al-

1 lows members of the public to identify indi-
2 vidual third-party collecting entities.

3 (B) For each registered third-party col-
4 lecting entity, the information described in
5 paragraph (2).

6 (C) A “Do Not Collect” registry link and
7 mechanism by which an individual may, after
8 the Commission has verified the identity of the
9 individual or individual’s parent or guardian,
10 which may include tokenization, easily submit a
11 request to all registered third-party collecting
12 entities that are not consumer reporting agen-
13 cies, and to the extent they are not acting as
14 consumer reporting agencies, as defined in sec-
15 tion 603(f) of the Fair Credit Reporting Act
16 (15 U.S.C. 1681a(f)) to—

17 (i) delete all covered data related to
18 such individual that the third-party col-
19 lecting entity did not collect from the indi-
20 vidual directly or when acting as a service
21 provider; and

22 (ii) ensure that any third-party col-
23 lecting entity no longer collects covered
24 data related to such individual without the
25 affirmative express consent of such indi-

1 vidual, except insofar as such covered enti-
2 ty is acting as a service provider. Each
3 third-party collecting entity that receives
4 such a request from an individual shall de-
5 lete all the covered data of the individual
6 not later than 30 days after the request is
7 received by the third-party collecting enti-
8 ty.

9 (c) PENALTIES.—A third-party collecting entity that
10 fails to register or provide the notice as required under
11 this section shall be liable for—

12 (1) a civil penalty of \$50 for each day it fails
13 to register or provide notice as required under this
14 subsection, not to exceed a total of \$10,000 for any
15 year; and

16 (2) an amount equal to the registration fees
17 due under paragraph (2) of subsection (b) for each
18 year that it failed to register as required under para-
19 graph (1) of such subsection.

20 **SEC. 207. CIVIL RIGHTS AND ALGORITHMS.**

21 (a) CIVIL RIGHTS PROTECTIONS.—

22 (1) IN GENERAL.—A covered entity or a service
23 provider may not collect, process, or transfer covered
24 data in a manner that discriminates in or otherwise
25 makes unavailable the equal enjoyment of goods or

1 services on the basis of race, color, religion, national
2 origin, sex, or disability.

3 (2) EXCEPTIONS.—This subsection shall not
4 apply to—

5 (A) the collection, processing, or transfer
6 of covered data for the purpose of—

7 (i) a covered entity's or a service pro-
8 vider's self-testing to prevent or mitigate
9 unlawful discrimination; or

10 (ii) diversifying an applicant, partici-
11 pant, or customer pool; or

12 (B) any private club or group not open to
13 the public, as described in section 201(e) of the
14 Civil Rights Act of 1964 (42 U.S.C. 2000a(e)).

15 (b) FTC ENFORCEMENT ASSISTANCE.—

16 (1) IN GENERAL.—Whenever the Commission
17 obtains information that a covered entity or service
18 provider may have collected, processed, or trans-
19 ferred covered data in violation of subsection (a), the
20 Commission shall transmit such information as al-
21 lowable under Federal law to any Executive agency
22 with authority to initiate enforcement actions or pro-
23 ceedings relating to such violation.

24 (2) ANNUAL REPORT.—Not later than 3 years
25 after the date of enactment of this Act, and annually

1 thereafter, the Commission shall submit to Congress
2 a report that includes a summary of—

3 (A) the types of information the Commis-
4 sion transmitted to Federal agencies under
5 paragraph (1) during the previous 1-year pe-
6 riod; and

7 (B) how such information relates to Fed-
8 eral civil rights laws.

9 (3) TECHNICAL ASSISTANCE.—In transmitting
10 information under paragraph (1), the Commission
11 may consult and coordinate with, and provide tech-
12 nical and investigative assistance, as appropriate, to
13 such Executive agency.

14 (4) COOPERATION WITH OTHER AGENCIES.—
15 The Commission may implement this subsection by
16 executing agreements or memoranda of under-
17 standing with the appropriate Federal agencies.

18 (c) ALGORITHM IMPACT AND EVALUATION.—

19 (1) ALGORITHM IMPACT ASSESSMENT.—

20 (A) IMPACT ASSESSMENT.—Notwith-
21 standing any other provision of law, not later
22 than 2 years after the date of enactment of this
23 Act, and annually thereafter, a large data hold-
24 er that uses an algorithm that may cause po-
25 tential harm to an individual, and uses such al-

1 gorithm solely or in part, to collect, process, or
2 transfer covered data must conduct an impact
3 assessment of such algorithm in accordance
4 with subparagraph (B).

5 (B) IMPACT ASSESSMENT SCOPE.—The im-
6 pact assessment required under subparagraph
7 (A) shall provide the following:

8 (i) A detailed description of the design
9 process and methodologies of the algo-
10 rithm.

11 (ii) A statement of the purpose, pro-
12 posed uses, and foreseeable capabilities
13 outside of the articulated proposed use of
14 the algorithm.

15 (iii) A detailed description of the data
16 used by the algorithm, including the spe-
17 cific categories of data that will be proc-
18 essed as input and any data used to train
19 the model that the algorithm relies on.

20 (iv) A description of the outputs pro-
21 duced by the algorithm.

22 (v) An assessment of the necessity
23 and proportionality of the algorithm in re-
24 lation to its stated purpose, including rea-
25 sons for the superiority of the algorithm

1 over nonautomated decision-making meth-
2 ods.

3 (vi) A detailed description of steps the
4 large data holder has taken or will take to
5 mitigate potential harms to individuals, in-
6 cluding potential harms related to—

7 (I) any individual under the age
8 of 17;

9 (II) making or facilitating adver-
10 tising for, or determining access to, or
11 restrictions on the use of housing,
12 education, employment, healthcare, in-
13 surance, or credit opportunities;

14 (III) determining access to, or re-
15 strictions on the use of, any place of
16 public accommodation, particularly as
17 such harms relate to the protected
18 characteristics of individuals, includ-
19 ing race, color, religion, national ori-
20 gin, sex, or disability; or

21 (IV) disparate impact on the
22 basis of individuals' race, color, reli-
23 gion, national origin, sex, or disability
24 status.

1 (2) ALGORITHM DESIGN EVALUATION.—Not-
2 withstanding any other provision of law, not later
3 than 2 years after the date of enactment of this Act,
4 a covered entity or service provider that knowingly
5 develops an algorithm, solely or in part, to collect,
6 process, or transfer covered data or publicly avail-
7 able information shall prior to deploying the algo-
8 rithm in interstate commerce evaluate the design,
9 structure, and inputs of the algorithm, including any
10 training data used to develop the algorithm, to re-
11 duce the risk of the potential harms identified under
12 paragraph (1)(B).

13 (3) OTHER CONSIDERATIONS.—

14 (A) FOCUS.—In complying with paragraph
15 (1) or (2), a covered entity and a service pro-
16 vider may focus the impact assessment or eval-
17 uation on any algorithm, or portions of an algo-
18 rithm, that may reasonably contribute to the
19 risk of the potential harms identified under
20 paragraph (1)(B).

21 (B) EXTERNAL, INDEPENDENT AUDITOR
22 OR RESEARCHER.—To the extent possible, a
23 covered entity and a service provider shall uti-
24 lize an external, independent auditor or re-
25 searcher to conduct an impact assessment

1 under paragraph (1) or an evaluation under
2 paragraph (2).

3 (C) AVAILABILITY.—

4 (i) IN GENERAL.—A covered entity
5 and a service provider—

6 (I) shall, not later than 30 days
7 after completing an impact assess-
8 ment or evaluation, submit the impact
9 assessment and evaluation conducted
10 under paragraphs (1) and (2) to the
11 Commission;

12 (II) shall, upon request, make
13 such impact assessment and evalua-
14 tion available to Congress; and

15 (III) may make a summary of
16 such impact assessment and evalua-
17 tion publicly available in a place that
18 is easily accessible to individuals.

19 (ii) TRADE SECRETS.—Covered enti-
20 ties and service providers must make all
21 submissions under this section to the Com-
22 mission in unredacted form, but a covered
23 entity and a service provider may redact
24 and segregate any trade secrets (as defined
25 in section 1839 of title 18, United States

1 Code) from public disclosure under this
2 subparagraph.

3 (D) ENFORCEMENT.—The Commission
4 may not use any information obtained solely
5 and exclusively through a covered entity or a
6 service provider’s disclosure of information to
7 the Commission in compliance with this section
8 for any purpose other than enforcing this Act,
9 including the study and report provisions in
10 paragraph 6 of this section. This provision shall
11 not preclude the Commission from providing
12 this information to Congress in response to a
13 subpoena or official Congressional request.

14 (4) GUIDANCE.—Not later than 2 years after
15 the date of enactment of this Act, the Commission
16 shall, in consultation with the Secretary of Com-
17 merce, or their respective designees, publish guid-
18 ance regarding compliance with this section.

19 (5) RULEMAKING AND EXEMPTION.—The Com-
20 mission shall have authority under section 553 of
21 title 5, United States Code, to promulgate regula-
22 tions as necessary to establish processes by which a
23 large data holder—

1 (A) shall submit an impact assessment to
2 the Commission under paragraph (3)(C)(i)(I);
3 and

4 (B) may exclude from this subsection any
5 algorithm that presents low or minimal risk for
6 potential for harms to individuals (as identified
7 under paragraph (1)(B)).

8 (6) STUDY AND REPORT.—

9 (A) STUDY.—The Commission, in con-
10 sultation with the Secretary of Commerce or
11 the Secretary's designee, shall conduct a study,
12 to review any impact assessment or evaluation
13 submitted under this paragraph. Such study
14 shall include an examination of—

15 (i) best practices for the assessment
16 and evaluation of algorithms; and

17 (ii) methods to reduce the risk of
18 harm to individuals that may be related to
19 the use of algorithms.

20 (B) REPORT.—

21 (i) INITIAL REPORT.—Not later than
22 3 years after the date of enactment of this
23 Act, the Commission, in consultation with
24 the Secretary of Commerce or the Sec-
25 retary's designee, shall submit to Congress

1 a report containing the results of the study
2 conducted under subsection (a), together
3 with recommendations for such legislation
4 and administrative action as the Commis-
5 sion determines appropriate.

6 (ii) ADDITIONAL REPORTS.—Not later
7 than 3 years after submission of the initial
8 report under clause (i), and as the Com-
9 mission determines necessary thereafter,
10 the Commission shall submit to Congress
11 an updated version of such report.

12 **SEC. 208. DATA SECURITY AND PROTECTION OF COVERED**
13 **DATA.**

14 (a) ESTABLISHMENT OF DATA SECURITY PRAC-
15 TICES.—

16 (1) IN GENERAL.—A covered entity or service
17 provider shall establish, implement, and maintain
18 reasonable administrative, technical, and physical
19 data security practices and procedures to protect
20 and secure covered data against unauthorized access
21 and acquisition.

22 (2) CONSIDERATIONS.—The reasonable admin-
23 istrative, technical, and physical data security prac-
24 tices required under paragraph (1) shall be appro-
25 priate to—

1 (A) the size and complexity of the covered
2 entity or service provider;

3 (B) the nature and scope of the covered
4 entity or the service provider's collecting, proc-
5 essing, or transferring of covered data;

6 (C) the volume and nature of the covered
7 data collected, processed, or transferred by the
8 covered entity or service provider;

9 (D) the sensitivity of the covered data col-
10 lected, processed, or transferred;

11 (E) the current state of the art in adminis-
12 trative, technical, and physical safeguards for
13 protecting such covered data; and

14 (F) the cost of available tools to improve
15 security and reduce vulnerabilities to unauthor-
16 ized access and acquisition of such covered data
17 in relation to the risks and nature of the cov-
18 ered data.

19 (b) SPECIFIC REQUIREMENTS.—The data security
20 practices required under subsection (a) shall include, at
21 a minimum, the following practices:

22 (1) ASSESS VULNERABILITIES.—Identifying
23 and assessing any material internal and external
24 risk to, and vulnerability in, the security of each sys-
25 tem maintained by the covered entity that collects,

1 processes, or transfers covered data, or service pro-
2 vider that collects, processes, or transfers covered
3 data on behalf of the covered entity, including unau-
4 thorized access to or risks to such covered data,
5 human vulnerabilities, access rights, and the use of
6 service providers. With respect to large data holders,
7 such activities shall include a plan to receive and re-
8 spond to unsolicited reports of vulnerabilities by any
9 entity or individual.

10 (2) PREVENTIVE AND CORRECTIVE ACTION.—
11 Taking preventive and corrective action designed to
12 mitigate any reasonably foreseeable risks or
13 vulnerabilities to covered data identified by the cov-
14 ered entity or service provider, consistent with the
15 nature of such risk or vulnerability, which may in-
16 clude implementing administrative, technical, or
17 physical safeguards or changes to data security prac-
18 tices or the architecture, installation, or implementa-
19 tion of network or operating software, among other
20 actions.

21 (3) EVALUATION OF PREVENTIVE AND CORREC-
22 TIVE ACTION.—Evaluating and making reasonable
23 adjustments to the safeguards described in para-
24 graph (2) in light of any material changes in tech-
25 nology, internal or external threats to covered data,

1 and the covered entity or service provider's own
2 changing business arrangements or operations.

3 (4) INFORMATION RETENTION AND DIS-
4 POSAL.—Disposing of covered data that is required
5 to be deleted by law or is no longer necessary for the
6 purpose for which the data was collected, processed,
7 or transferred, unless an individual has provided af-
8 firmative express consent to such retention. Such
9 disposal shall include destroying, permanently eras-
10 ing, or otherwise modifying the covered data to
11 make such data permanently unreadable or indeci-
12 pherable and unrecoverable to ensure ongoing com-
13 pliance with this section.

14 (5) TRAINING.—Training each employee with
15 access to covered data on how to safeguard covered
16 data and updating such training as necessary.

17 (6) DESIGNATION.—Designating an officer, em-
18 ployee, or employees to maintain and implement
19 such practices.

20 (7) INCIDENT RESPONSE.—Implementing pro-
21 cedures to detect, respond to, or recover from secu-
22 rity incidents or breaches.

23 (c) REGULATIONS.—The Commission may promul-
24 gate in accordance with section 553 of title 5, United

1 States Code, technology-neutral regulations to establish
2 processes for complying with this section.

3 (d) APPLICABILITY OF OTHER INFORMATION SECUR-
4 RITY LAWS.—A covered entity that is required to comply
5 with title V of the Gramm-Leach-Bliley Act (15 U.S.C.
6 6801 et seq.) or the Health Information Technology for
7 Economic and Clinical Health Act (42 U.S.C. 17931 et
8 seq.), and is in compliance with the information security
9 requirements of such Act as determined by the enforce-
10 ment authority in such Act, shall be deemed to be in com-
11 pliance with the requirements of this section with respect
12 to any data covered by such information security require-
13 ments.

14 **SEC. 209. SMALL BUSINESS PROTECTIONS.**

15 (a) IN GENERAL.—

16 (1) Any covered entity or service provider that
17 can establish that it met the requirements described
18 in paragraph (2) for the period of the 3 preceding
19 calendar years (or for the period during which the
20 covered entity has been in existence if such period
21 is less than 3 years) shall—

22 (A) be exempt from compliance with sec-
23 tions 203(a)(4), 208(b)(1)–(3), (5)–(7), and
24 301(c); and

1 (B) at the covered entity's sole discretion,
2 have the option of complying with section
3 203(a)(2) by, after receiving a verified request
4 from an individual to correct covered data of
5 the individual under such section, deleting such
6 covered data in its entirety instead of making
7 the requested correction.

8 (2) EXEMPTION REQUIREMENTS.—The require-
9 ments of this paragraph are, with respect to a cov-
10 ered entity or a service provider and a period, the
11 following:

12 (A) The covered entity or service provider's
13 average annual gross revenues during the pe-
14 riod did not exceed \$41,000,000.

15 (B) The covered entity or service provider,
16 on average, did not annually collect or process
17 the covered data of more than 200,000 individ-
18 uals during the period beyond the purpose of
19 initiating, rendering, billing for, finalizing, com-
20 pleting, or otherwise collecting payment for a
21 requested service or product, so long as all cov-
22 ered data for such purpose is deleted or de-
23 identified within 90 days.

24 (C) The covered entity or service provider
25 did not derive more than 50 percent of its rev-

1 enue from transferring covered data during any
2 year (or part of a year if the covered entity has
3 been in existence for less than 1 year) that oc-
4 curs during the period.

5 (3) DEFINITION.—For purposes of this section,
6 the term “revenue” as it relates to any covered enti-
7 ty that is not organized to carry on business for its
8 own profit or that of their members, means the
9 gross receipts the covered entity received in whatever
10 form from all sources without subtracting any costs
11 or expenses, and includes contributions, gifts,
12 grants, dues or other assessments, income from in-
13 vestments, or proceeds from the sale of real or per-
14 sonal property.

15 (4) JOURNALISM.—Nothing in this Act shall be
16 construed to limit or diminish First Amendment
17 freedoms to gather and publish information guaran-
18 teed under the Constitution.

19 **SEC. 210. UNIFIED OPT-OUT MECHANISMS.**

20 For the rights established under sections 204(b) and
21 (c), and section 206(c)(3)(D) not later than 18 months
22 after the date of enactment of this Act, the Commission
23 shall establish one or more acceptable privacy protective,
24 centralized mechanisms, including global privacy signals
25 such as browser or device privacy settings, for individuals

1 to exercise all such rights through a single interface for
2 a covered entity to utilize to allow an individual to make
3 such opt out designations with respect to covered data re-
4 lated to such individual.

5 **TITLE III—CORPORATE** 6 **ACCOUNTABILITY**

7 **SEC. 301. EXECUTIVE RESPONSIBILITY.**

8 (a) IN GENERAL.—Beginning 1 year after the date
9 of enactment of this Act, an executive officer of a large
10 data holder shall annually certify, in good faith, to the
11 Commission, in a manner specified by the Commission by
12 regulation under section 553 of title 5, United States
13 Code, that the entity maintains—

14 (1) internal controls reasonably designed to
15 comply with this Act; and

16 (2) reporting structures to ensure that such
17 certifying officers are involved in, and are respon-
18 sible for, decisions that impact the entity's compli-
19 ance with this Act.

20 (b) REQUIREMENTS.—A certification submitted
21 under subsection (a) shall be based on a review of the ef-
22 fectiveness of a large data holder's internal controls and
23 reporting structures that is conducted by the certifying of-
24 ficers not more than 90 days before the submission of the
25 certification.

1 (c) DESIGNATION OF PRIVACY AND DATA SECURITY
2 OFFICER.—

3 (1) IN GENERAL.—A covered entity and a serv-
4 ice provider shall designate—

5 (A) 1 or more qualified employees as pri-
6 vacy officers; and

7 (B) 1 or more qualified employees (in addi-
8 tion to any employee designated under subpara-
9 graph (A)) as data security officers.

10 (2) REQUIREMENTS FOR OFFICERS.—An em-
11 ployee who is designated by a covered entity or a
12 service provider as a privacy officer or a data secu-
13 rity officer shall, at a minimum—

14 (A) implement a data privacy program and
15 data security program to safeguard the privacy
16 and security of covered data in compliance with
17 the requirements of this Act; and

18 (B) facilitate the covered entity or service
19 provider’s ongoing compliance with this Act.

20 (3) ADDITIONAL REQUIREMENTS FOR LARGE
21 DATA HOLDERS.—A large data holder shall des-
22 ignate at least 1 of the officers described in para-
23 graph (1) of this subsection to report directly to the
24 highest official at the large data holder as a privacy
25 protection officer who shall, in addition to the re-

1 requirements in paragraph (2), either directly or
2 through a supervised designee or designees—

3 (A) establish processes to periodically re-
4 view and update the privacy and security poli-
5 cies, practices, and procedures of the large data
6 holder, as necessary;

7 (B) conduct biennial and comprehensive
8 audits to ensure the policies, practices, and pro-
9 cedures of the large data holder work to ensure
10 the company is in compliance with all applicable
11 laws and ensure such audits are accessible to
12 the Commission upon such request;

13 (C) develop a program to educate and
14 train employees about compliance requirements;

15 (D) maintain updated, accurate, clear, and
16 understandable records of all privacy and data
17 security practices undertaken by the large data
18 holder; and

19 (E) serve as the point of contact between
20 the large data holder and enforcement authori-
21 ties.

22 (d) LARGE DATA HOLDER PRIVACY IMPACT ASSESS-
23 MENTS.—

24 (1) IN GENERAL.—Not later than 1 year after
25 the date of enactment of this Act or 1 year after the

1 date that a covered entity or service provider first
2 meets the definition of large data holder, whichever
3 is earlier, and biennially thereafter, each large data
4 holder shall conduct a privacy impact assessment
5 that weighs the benefits of the large data holder's
6 covered data collecting, processing, and transfer
7 practices against the potential adverse consequences
8 of such practices to individual privacy.

9 (2) ASSESSMENT REQUIREMENTS.—A privacy
10 impact assessment required under paragraph (1)
11 shall be—

12 (A) reasonable and appropriate in scope
13 given—

14 (i) the nature of the covered data col-
15 lected, processed, and transferred by the
16 large data holder;

17 (ii) the volume of the covered data
18 collected, processed, and transferred by the
19 large data holder; and

20 (iii) the potential risks posed to the
21 privacy of individuals by the collecting,
22 processing, and transfer of covered data by
23 the large data holder;

24 (B) documented in written form and main-
25 tained by the large data holder unless rendered

out of date by a subsequent assessment conducted under paragraph (1); and

(C) approved by the privacy protection officer designated in subsection (c)(3) of the large data holder.

(3) **ADDITIONAL FACTORS TO INCLUDE IN ASSESSMENT.**—In assessing the privacy risks, including substantial privacy risks, the large data holder may include reviews of the means by which technologies, including blockchain and distributed ledger technologies and other emerging technologies, are used to secure covered data.

SEC. 302. SERVICE PROVIDERS AND THIRD PARTIES.

(a) **SERVICE PROVIDERS.**—A service provider—

(1) shall only collect, process, and transfer service provider data to the extent strictly necessary and proportionate to provide a service requested by the covered entity. This paragraph shall not require a service provider to collect or process covered data if the service provider would not otherwise do so;

(2) shall not collect, process, or transfer service provider data if the service provider has actual knowledge that the covered entity violated this Act with respect to such data;

1 (3) shall assist a covered entity in fulfilling the
2 covered entity's obligation to respond to individual
3 rights requests pursuant to section 203, by appropriate technical and organizational measures, taking
4 into account the nature of the processing and the in-
5 formation reasonably available to the service pro-
6 vider;
7

8 (4) may engage another service provider for
9 purposes of processing service provider data on be-
10 half of a covered entity only after providing the cov-
11 ered entity that is directing the services or functions
12 of the service provider with respect to such service
13 provider data with notice, and pursuant to a written
14 contract that requires such other service provider to
15 satisfy the obligations of the service provider with
16 respect to such service provider data;

17 (5) shall upon the reasonable request of the
18 covered entity, make available to the covered entity
19 information necessary to demonstrate the service
20 provider's compliance with the obligations in this
21 Act, which may include making available a report of
22 an independent assessment arranged by the service
23 provider on terms agreed to by the parties and mak-
24 ing the report required under section 207(c)(2) as
25 applicable;

1 (6) shall, at the covered entity's direction, de-
2 lete or return all covered data to the covered entity
3 as requested at the end of the provision of services,
4 unless retention of the covered data is required by
5 law;

6 (7) shall not transfer service provider data to
7 any person with the exception of another service pro-
8 vider without the affirmative express consent, ob-
9 tained by the covered entity with the direct relation-
10 ship to the individual that is directing the services
11 or functions of the service provider with respect to
12 the service provider data, of the individual to whom
13 the service provider data is linked or reasonably
14 linkable;

15 (8) shall develop, implement, and maintain rea-
16 sonable administrative, technical, and physical safe-
17 guards that are designed to protect the security and
18 confidentiality of covered data it processes consistent
19 with section 208; and

20 (9) shall be exempt from the requirements of
21 section 202(d) with respect to service provider data
22 but shall provide direct notification regarding mate-
23 rial changes to its privacy policy to each covered en-
24 tity with which it provides services or functions as
25 a service provider, in each language that the privacy

1 policy is made available. Compliance with this provi-
2 sion does not alleviate any obligations the service
3 provider has to the covered entity to which it pro-
4 vides services or functions as a service provider.

5 (b) CONTRACTS BETWEEN COVERED ENTITIES AND
6 SERVICE PROVIDERS.—A person or entity may act as a
7 service provider pursuant to a written contract between
8 the covered entity and the service provider, or a written
9 contract between one service provider and a second service
10 provider as permitted in section 302(a)(4), provided that
11 the contract—

12 (1) governs the service provider’s data proc-
13 essing procedures with respect to processing or
14 transfer performed on behalf of the covered entity or
15 service provider;

16 (2) clearly sets forth—

17 (A) instructions for processing data;

18 (B) the nature and purpose of processing;

19 (C) the type of data subject to processing;

20 (D) the duration of processing; and

21 (E) the rights and obligations of both par-
22 ties;

23 (3) does not relieve a covered entity or a service
24 provider of an obligation under this Act; and

25 (4) prohibits—

1 (A) collecting, processing, or transferring
2 covered data in contravention to subsection (a);
3 and

4 (B) combining service provider data with
5 covered data which the service provider receives
6 from or on behalf of another person or persons
7 or collects from its own interaction with an in-
8 dividual. The contract may, subject to agree-
9 ment with the service provider, permit a covered
10 entity to monitor the service provider's compli-
11 ance with the contract through measures in-
12 cluding, but not limited to, ongoing manual re-
13 views and automated scans, and regular assess-
14 ments, audits, or other technical and oper-
15 ational testing at least once every 12 months.

16 (c) RELATIONSHIP BETWEEN COVERED ENTITIES
17 AND SERVICE PROVIDERS.—

18 (1) Determining whether a person is acting as
19 a covered entity or service provider with respect to
20 a specific processing of data is a fact-based deter-
21 mination that depends upon the context in which
22 such data is processed.

23 (2) A covered entity or service provider that
24 transfers covered data to a service provider, in com-
25 pliance with the requirements of this Act, is not lia-

1 ble for a violation of this Act by the service provider
2 to whom such covered data was transferred, this Act
3 provided that, at the time of transferring such cov-
4 ered data, the covered entity or service provider did
5 not know or have reason to know that the service
6 provider would likely commit a violation of this Act.

7 (3) A covered entity or service provider that re-
8 ceives covered data in compliance with the require-
9 ments of this Act is not in violation of this Act as
10 a result of a violation by a covered entity or service
11 provider from which it receives such covered data.

12 (d) THIRD PARTIES.—A third party—

13 (1) shall not process third-party data for a
14 processing purpose other than, in the case of sen-
15 sitive covered data, the processing purpose for which
16 the individual gave affirmative express consent and,
17 in the case of non-sensitive data, the processing pur-
18 pose for which the covered entity made a disclosure
19 pursuant to section 204(b)(4);

20 (2) for purposes of paragraph (1), may reason-
21 ably rely on representations made by the covered en-
22 tity that transferred the third-party data, provided
23 that the third party conducts reasonable due dili-
24 gence on the representations of the covered entity
25 and finds those representations to be credible; and

1 (3) shall be exempt from the requirements of
2 section 204 with respect to third-party data, but
3 shall otherwise have the same responsibilities and
4 obligations as a covered entity with respect to such
5 data under all other provisions of this Act.

6 (e) ADDITIONAL OBLIGATIONS ON COVERED ENTI-
7 TIES.—

8 (1) IN GENERAL.—A covered entity or service
9 provider shall exercise reasonable due diligence in—
10 (A) selecting a service provider; and
11 (B) deciding to transfer covered data to a
12 third party.

13 (2) GUIDANCE.—Not later than 2 years after
14 the date of enactment of this Act, the Commission
15 shall publish guidance regarding compliance with
16 this subsection, taking into consideration the bur-
17 dens on small- and medium-sized covered entities.

18 **SEC. 303. TECHNICAL COMPLIANCE PROGRAMS.**

19 (a) IN GENERAL.—Not later than 1 year after the
20 date of the enactment of this Act, the Commission shall
21 promulgate regulations under section 553 of title 5,
22 United States Code, to establish a process for the proposal
23 and approval of technical compliance programs under this
24 section specific to any technology, product, service, or

1 method used by a covered entity to collect, process, or
2 transfer covered data.

3 (b) SCOPE OF PROGRAMS.—The technical compliance
4 programs established under this section shall, with respect
5 to a technology, product, service, or method used by a cov-
6 ered entity to collect, process, or transfer covered data—

7 (1) establish guidelines for compliance with this
8 Act;

9 (2) meet or exceed the requirements of this Act;
10 and

11 (3) be made publicly available to any individual
12 whose covered data is collected, processed, or trans-
13 ferred using such technology, product, service, or
14 method.

15 (c) APPROVAL PROCESS.—

16 (1) IN GENERAL.—Any request for approval,
17 amendment, or repeal of a technical compliance pro-
18 gram may be submitted to the Commission by any
19 person, including a covered entity, a representative
20 of a covered entity, an association of covered enti-
21 ties, or a public interest group or organization.
22 Within 90 days, the Commission shall publish the
23 request and provide an opportunity for public com-
24 ment on the proposal.

1 (2) EXPEDITED RESPONSE TO REQUESTS.—Be-
2 ginning 1 year after the date of enactment of this
3 Act, the Commission shall act upon a request for the
4 proposal and approval of a technical compliance pro-
5 gram not later than 180 days after the filing of the
6 request, and shall set forth publicly in writing its
7 conclusions with regard to such request.

8 (d) RIGHT TO APPEAL.—Final action by the Com-
9 mission on a request for approval, amendment, or repeal
10 of a technical compliance program, or the failure to act
11 within the 180 day period after a request for approval,
12 amendment, or repeal of a technical compliance program
13 is made under subsection (c), may be appealed to a Fed-
14 eral district court of the United States of appropriate ju-
15 risdiction as provided for in section 702 of title 5, United
16 States Code.

17 (e) EFFECT ON ENFORCEMENT.—

18 (1) IN GENERAL.—Prior to commencing an in-
19 vestigation or enforcement action against any cov-
20 ered entity under this Act, the Commission and
21 State attorney general shall consider the covered en-
22 tity's history of compliance with any technical com-
23 pliance program approved under this section and
24 any action taken by the covered entity to remedy
25 noncompliance with such program. If such enforce-

1 ment action described in Sec. 403 is commenced, the
2 covered entity's history of compliance with any tech-
3 nical compliance program approved under this sec-
4 tion and any action taken by the covered entity to
5 remedy noncompliance with such program shall be
6 taken into consideration when determining liability
7 or a penalty. The covered entity's history of compli-
8 ance with any technical compliance program shall
9 not affect any burden of proof or the weight given
10 to evidence in an enforcement or judicial proceeding.

11 (2) COMMISSION AUTHORITY.—Approval of a
12 technical compliance program shall not limit the au-
13 thority of the Commission, including the Commis-
14 sion's authority to commence an investigation or en-
15 forcement action against any covered entity under
16 this Act or any other Act.

17 (3) RULE OF CONSTRUCTION.—Nothing in this
18 subsection shall provide any individual, class of indi-
19 viduals, or person with any right to seek discovery
20 of any non-public Commission deliberations or activi-
21 ties or impose any pleading requirement on the
22 Commission should it bring an enforcement action of
23 any kind.

1 **SEC. 304. COMMISSION APPROVED COMPLIANCE GUIDE-**
2 **LINES.**

3 (a) APPLICATION FOR COMPLIANCE GUIDELINE AP-
4 PROVAL.—

5 (1) IN GENERAL.—A covered entity that is not
6 a third-party collecting entity and meets the require-
7 ments of section 209, or a group of such covered en-
8 tities, may apply to the Commission for approval of
9 1 or more sets of compliance guidelines governing
10 the collection, processing, and transfer of covered
11 data by the covered entity or group of covered enti-
12 ties.

13 (2) APPLICATION REQUIREMENTS.—Such appli-
14 cation shall include—

15 (A) a description of how the proposed
16 guidelines will meet or exceed the requirements
17 of this Act;

18 (B) a description of the entities or activi-
19 ties the proposed set of compliance guidelines is
20 designed to cover;

21 (C) a list of the covered entities that meet
22 the requirements of section 209 and are not
23 third-party collecting entities, if any are known
24 at the time of application, that intend to adhere
25 to the compliance guidelines; and

1 (D) a description of how such covered enti-
2 ties will be independently assessed for adher-
3 ence to such compliance guidelines, including
4 the independent organization not associated
5 with any of the covered entities that may par-
6 ticipate in guidelines that will administer such
7 guidelines.

8 (3) COMMISSION REVIEW.—

9 (A) INITIAL APPROVAL.—

10 (i) PUBLIC COMMENT PERIOD.—With-
11 in 90 days after the receipt of proposed
12 guidelines submitted pursuant to para-
13 graph (2), the Commission shall publish
14 the proposal and provide an opportunity
15 for public comment on such compliance
16 guidelines.

17 (ii) APPROVAL.—The Commission
18 shall approve an application regarding pro-
19 posed guidelines under paragraph (2) if
20 the applicant demonstrates that the com-
21 pliance guidelines—

22 (I) meet or exceed requirements
23 of this Act;

24 (II) provide for the regular re-
25 view and validation by an independent

1 organization not associated with any
2 of the covered entities that may par-
3 ticipate in the guidelines and that is
4 approved by the Commission to con-
5 duct such reviews of the compliance
6 guidelines of the covered entity or en-
7 tities to ensure that the covered entity
8 or entities continue to meet or exceed
9 the requirements of this Act; and

10 (III) include a means of enforce-
11 ment if a covered entity does not meet
12 or exceed the requirements in the
13 guidelines, which may include referral
14 to the Commission for enforcement
15 consistent with section 401 or referral
16 to the appropriate State attorney gen-
17 eral for enforcement consistent with
18 section 402.

19 (iii) **TIMELINE.**—Within 1 year of re-
20 ceiving an application regarding proposed
21 guidelines under paragraph (2), the Com-
22 mission shall issue a determination approv-
23 ing or denying the application and pro-
24 viding its reasons for approving or denying
25 such application.

1 (B) APPROVAL OF MODIFICATIONS.—

2 (i) IN GENERAL.—If the independent
3 organization administering a set of guide-
4 lines makes material changes to guidelines
5 previously approved by the Commission,
6 the independent organization must submit
7 the updated guidelines to the Commission
8 for approval. As soon as feasible, the Com-
9 mission shall publish the updated guide-
10 lines and provide an opportunity for public
11 comment.

12 (ii) TIMELINE.—The Commission
13 shall approve or deny any material change
14 to the guidelines within 180 days after re-
15 ceipt of the submission for approval.

16 (b) WITHDRAWAL OF APPROVAL.—If at any time the
17 Commission determines that the guidelines previously ap-
18 proved no longer meet the requirements of this Act or a
19 regulation promulgated under this Act or that compliance
20 with the approved guidelines is insufficiently enforced by
21 the independent organization administering the guidelines,
22 the Commission shall notify the covered entities or group
23 of such entities and the independent organization of its
24 determination to withdraw approval of such guidelines and
25 the basis for doing so. Upon receipt of such notice, the

1 covered entity or group of such entities and the inde-
2 pendent organization may cure any alleged deficiency with
3 the guidelines or the enforcement of such guidelines within
4 180 days and submit the proposed cure or cures to the
5 Commission. If the Commission determines that such
6 cures eliminate the alleged deficiency in the guidelines,
7 then the Commission may not withdraw approval of such
8 guidelines on the basis of such determination.

9 (c) DEEMED COMPLIANCE.—A covered entity that is
10 eligible to participate under subsection (a)(1), and partici-
11 pates, in guidelines approved under this section shall be
12 deemed in compliance with the relevant provisions of this
13 Act if it is in compliance with such guidelines.

14 **SEC. 305. DIGITAL CONTENT FORGERIES.**

15 (a) REPORTS.—Not later than 1 year after the date
16 of enactment of this Act, and annually thereafter, the Sec-
17 retary of Commerce or the Secretary's designee shall pub-
18 lish a report regarding digital content forgeries.

19 (b) REQUIREMENTS.—Each report under subsection
20 (a) shall include the following:

21 (1) A definition of digital content forgeries
22 along with accompanying explanatory materials, ex-
23 cept that the definition developed pursuant to this
24 section shall not supersede any other provision of

1 law or be construed to limit the authority of any Ex-
2 ecutive agency related to digital content forgeries.

3 (2) A description of the common sources of dig-
4 ital content forgeries in the United States and com-
5 mercial sources of digital content forgery tech-
6 nologies.

7 (3) An assessment of the uses, applications, and
8 harms of digital content forgeries.

9 (4) An analysis of the methods and standards
10 available to identify digital content forgeries as well
11 as a description of the commercial technological
12 counter-measures that are, or could be, used to ad-
13 dress concerns with digital content forgeries, which
14 may include the provision of warnings to viewers of
15 suspect content.

16 (5) A description of the types of digital content
17 forgeries, including those used to commit fraud,
18 cause harm, or violate any provision of law.

19 (6) Any other information determined appro-
20 priate by the Secretary of Commerce or the Sec-
21 retary's designee.

1 **TITLE IV—ENFORCEMENT, AP-**
2 **PLICABILITY, AND MISCELLA-**
3 **NEOUS**

4 **SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COM-**
5 **MISSION.**

6 (a) NEW BUREAU.—

7 (1) IN GENERAL.—The Commission shall estab-
8 lish within the Commission a new bureau, the Bu-
9 reau of Privacy, which shall be comparable in struc-
10 ture, size, organization, and authority to the existing
11 Bureaus within the Commission related to consumer
12 protection and competition.

13 (2) MISSION.—The mission of the bureau es-
14 tablished under this subsection shall be to assist the
15 Commission in exercising the Commission’s author-
16 ity under this Act and related authorities.

17 (3) TIMELINE.—The bureau shall be estab-
18 lished, staffed, and fully operational not later than
19 1 year after the date of enactment of this Act.

20 (b) OFFICE OF BUSINESS MENTORSHIP.—The Direc-
21 tor of the Bureau established under subsection (a) shall
22 establish within the Bureau an Office of Business
23 Mentorship to provide guidance and education to covered
24 entities regarding compliance with this Act. Covered enti-
25 ties may request advice from the Commission or this office

1 with respect to a course of action which the covered entity
2 proposes to pursue and which may relate to the require-
3 ments of this Act.

4 (c) ENFORCEMENT BY THE FEDERAL TRADE COM-
5 MISSION.—

6 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
7 TICES.—A violation of this Act or a regulation pro-
8 mulgated under this Act shall be treated as a viola-
9 tion of a rule defining an unfair or deceptive act or
10 practice prescribed under section 18(a)(1)(B) of the
11 Federal Trade Commission Act (15 U.S.C.
12 57a(a)(1)(B)).

13 (2) POWERS OF THE COMMISSION.—

14 (A) IN GENERAL.—Except as provided in
15 paragraphs (3), (4), and (5), the Commission
16 shall enforce this Act and the regulations pro-
17 mulgated under this Act in the same manner,
18 by the same means, and with the same jurisdic-
19 tion, powers, and duties as though all applicable
20 terms and provisions of the Federal Trade
21 Commission Act (15 U.S.C. 41 et seq.) were in-
22 corporated into and made a part of this Act.

23 (B) PRIVILEGES AND IMMUNITIES.—Any
24 person who violates this Act or a regulation
25 promulgated under this Act shall be subject to

1 the penalties and entitled to the privileges and
2 immunities provided in the Federal Trade Com-
3 mission Act (15 U.S.C. 41 et seq.).

4 (3) LIMITING CERTAIN ACTIONS UNRELATED
5 TO THIS ACT.—If the Commission brings a civil ac-
6 tion under this Act alleging that an act or practice
7 violates this Act or a regulation promulgated under
8 this Act, the Commission may not seek a cease and
9 desist order against the same defendant under sec-
10 tion 5(b) of the Federal Trade Commission Act (15
11 U.S.C. 45(b)) to stop that same act or practice on
12 the grounds that such act or practice constitutes an
13 unfair or deceptive act or practice.

14 (4) COMMON CARRIERS AND NONPROFITS.—
15 Notwithstanding any jurisdictional limitation of the
16 Commission with respect to consumer protection or
17 privacy, the Commission shall enforce this Act and
18 the regulations promulgated under this Act, in the
19 same manner provided in subsections (1), (2), (3),
20 and (5) of this subsection, with respect to common
21 carriers subject to the Communications Act of 1934
22 (47 U.S.C. 151 et seq.) and All Acts amendatory
23 thereof and supplementary thereto; and organiza-
24 tions not organized to carry on business for their
25 own profit or that of their members.

1 (5) DATA PRIVACY AND SECURITY VICTIMS RE-
2 LIEF FUND.—

3 (A) ESTABLISHMENT OF VICTIMS RELIEF
4 FUND.—There is established in the Treasury of
5 the United States a separate fund to be known
6 as the “Privacy and Security Victims Relief
7 Fund” (referred to in this paragraph as the
8 “Victims Relief Fund”).

9 (B) DEPOSITS.—The amount of any civil
10 penalty obtained against any covered entity or
11 service provider or any other relief ordered to
12 provide redress, payments or compensation, or
13 other monetary relief to individuals that cannot
14 be located or the payment of which would other-
15 wise not be practicable in any judicial or admin-
16 istrative action to enforce this Act or a regula-
17 tion promulgated under this Act shall be depos-
18 ited into the Victims Relief Fund.

19 (C) USE OF FUND AMOUNTS.—

20 (i) AVAILABILITY TO THE COMMIS-
21 SION.—Notwithstanding section 3302 of
22 title 31, United States Code, amounts in
23 the Victims Relief Fund shall be available
24 to the Commission, without fiscal year lim-
25 itation, to provide redress, payments or

1 compensation, or other monetary relief to
2 individuals affected by an act or practice
3 for which relief has been obtained under
4 this Act.

5 (ii) OTHER PERMISSIBLE USES.—To
6 the extent that individuals cannot be lo-
7 cated or such redress, payments or com-
8 pensation, or other monetary relief are oth-
9 erwise not practicable, the Commission
10 may use such funds for the purpose of—

11 (I) funding the activities of the
12 Office of Business Mentorship estab-
13 lished under subsection (b); or

14 (II) engaging in technological re-
15 search that the Commission considers
16 necessary to enforce or administer
17 this Act.

18 **SEC. 402. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

19 (a) CIVIL ACTION.—In any case in which the attor-
20 ney general of a State or State Privacy Authority has rea-
21 son to believe that an interest of the residents of that
22 State has been, may be, or is adversely affected by the
23 engagement of any a covered entity or service provider in
24 an act or practice that has violated this Act or a regulation
25 promulgated under this Act, the attorney general of the

1 State, or State Privacy Authority, may bring a civil action
2 in the name of the State, or as *parens patriae* on behalf
3 of the residents of the State. Any such action shall be
4 brought exclusively in an appropriate Federal district
5 court of the United States to—

6 (1) enjoin that act or practice;

7 (2) enforce compliance with this Act or the reg-
8 ulation;

9 (3) obtain damages, civil penalties, restitution,
10 or other compensation on behalf of the residents of
11 the State; or

12 (4) reasonable attorneys' fees and other litiga-
13 tion costs reasonably incurred.

14 (b) RIGHTS OF THE COMMISSION.—

15 (1) IN GENERAL.—Except where not feasible,
16 the attorney general of a State or State Privacy Au-
17 thority shall notify the Commission in writing prior
18 to initiating a civil action under subsection (a). Such
19 notice shall include a copy of the complaint to be
20 filed to initiate such action. Upon receiving such no-
21 tice, the Commission may intervene in such action as
22 of right pursuant to the Federal Rules of Civil Pro-
23 cedure.

24 (2) NOTIFICATION TIMELINE.—Where it is not
25 feasible for the attorney general of a State or State

1 Privacy Authority to provide the notification re-
2 quired by paragraph (1) before initiating a civil ac-
3 tion under subsection (a), the attorney general of a
4 State or State Privacy Authority shall notify the
5 Commission immediately after initiating the civil ac-
6 tion.

7 (c) ACTIONS BY THE COMMISSION.—In any case in
8 which a civil action is instituted by or on behalf of the
9 Commission for violation of this Act or a regulation pro-
10 mulgated under this Act, no attorney general or State Pri-
11 vacy Authority may, during the pendency of such action,
12 institute a civil action against any defendant named in the
13 complaint in the action instituted by or on behalf of the
14 Commission for violation of this Act or a regulation pro-
15 mulgated under this Act that is alleged in such complaint,
16 if the Commission’s complaint alleges such violations af-
17 fected the residents of the relevant State or individuals
18 nationwide. In a case brought by the Commission that af-
19 fects the interests of a State, an attorney general of such
20 State or State Privacy Authority may intervene as of right
21 pursuant to the Federal Rules of Civil Procedure.

22 (d) RULE OF CONSTRUCTION.—Nothing in this sec-
23 tion shall be construed to prevent the attorney general of
24 a State or State Privacy Authority from exercising the
25 powers conferred on the attorney general or State Privacy

1 Authority to conduct investigations, to administer oaths
2 or affirmations, or to compel the attendance of witnesses
3 or the production of documentary or other evidence.

4 (e) PRESERVATION OF STATE POWERS.—Except as
5 provided in subsection (c), no provision of this section
6 shall be construed as altering, limiting, or affecting the
7 authority of a State attorney general or State Privacy Au-
8 thority to—

9 (1) bring an action or other regulatory pro-
10 ceeding arising solely under the laws in effect in that
11 State; or

12 (2) exercise the powers conferred on the attor-
13 ney general or State Privacy Authority by the laws
14 of the State, including the ability to conduct inves-
15 tigations, administer oaths or affirmations, or com-
16 pel the attendance of witnesses or the production of
17 documentary or other evidence.

18 **SEC. 403. ENFORCEMENT BY INDIVIDUALS.**

19 (a) ENFORCEMENT BY INDIVIDUALS.—

20 (1) IN GENERAL.—Beginning 4 years after the
21 date on which this Act takes effect, any individual
22 who suffers an injury that could be addressed by the
23 relief permitted in paragraph (2) for a violation of
24 this Act or a regulation promulgated under this Act
25 by a covered entity may bring a civil action against

1 such entity in any Federal court of competent juris-
2 diction.

3 (2) RELIEF.—In a civil action brought under
4 paragraph (1) in which the plaintiff prevails, the
5 court may award the plaintiff—

6 (A) an amount equal to the sum of any ac-
7 tual damages sustained;

8 (B) injunctive relief; and

9 (C) reasonable attorney's fees and litiga-
10 tion costs.

11 (3) RIGHTS OF THE COMMISSION AND STATE
12 ATTORNEYS GENERAL.—

13 (A) IN GENERAL.—Prior to an individual
14 bringing a civil action under paragraph (1),
15 such individual must first notify the Commis-
16 sion and the attorney general of the State of
17 the individuals residence in writing outlining
18 their desire to commence a civil action. Upon
19 receiving such notice, the Commission and
20 State attorney general shall make a determina-
21 tion, not later than 60 days after receiving such
22 notice, as to whether they will independently
23 seek to intervene in such action, and upon in-
24 tervening—

1 (i) be heard on all matters arising in
2 such action; and

3 (ii) file petitions for appeal of a deci-
4 sion in such action.

5 (B) BAD FAITH.—Any written communica-
6 tion requesting a monetary payment that is
7 sent to a covered entity shall be considered to
8 have been sent in bad faith and shall be unlaw-
9 ful as defined in this Act, if the written commu-
10 nication was sent:

11 (i) Prior to the date that is 60 days
12 after either a State attorney general or the
13 Commission has received the notice re-
14 quired under subparagraph (A).

15 (ii) After the Commission or attorney
16 general of a State made the determination
17 to independently seek civil actions against
18 such entity as outlined in subparagraph
19 (A).

20 (4) FTC STUDY.—Beginning on the date that
21 is 5 years after the date of enactment of this Act,
22 the Commission's Bureau of Economics shall con-
23 duct an annual study to determine the economic im-
24 pacts in the United States of demand letters and the
25 scope of the rights of an individual to bring forth

1 civil actions against covered entities. Such study
2 shall include, but not be limited to include the fol-
3 lowing:

4 (A) The impact on increasing insurance
5 rates in the United States.

6 (B) The impact on the ability of covered
7 entities to offer new products or services.

8 (C) The impact on the creation and growth
9 of startup companies, including tech startup
10 companies.

11 (D) Any emerging risks and long-term
12 trends in relevant marketplaces, supply chains,
13 and labor availability.

14 (5) REPORT TO CONGRESS.—Not later than 1
15 year after the first day on which individuals are able
16 to bring civil actions under this subsection, and an-
17 nually thereafter, the Commission shall submit to
18 the Committee on Energy and Commerce of the
19 House of Representatives and the Committee on
20 Commerce, Science, and Transportation of the Sen-
21 ate a report that contains the results of the study
22 conducted under paragraph (4).

23 (b) PRE-DISPUTE ARBITRATION AGREEMENTS AND
24 PRE-DISPUTE JOINT-ACTION WAIVERS RELATED TO IN-
25 DIVIDUALS UNDER THE AGE OF 18.—

1 (1) ARBITRATION.—Except as provided in sec-
2 tion 303(d), and notwithstanding any other provi-
3 sion of law, no agreement for pre-dispute arbitration
4 with respect to an individual under the age of 18
5 may limit any of the rights provided in this Act.

6 (2) JOINT-ACTION WAIVERS.—Notwithstanding
7 any other provision of law, no agreement for pre-dis-
8 pute joint-action waiver with respect to an individual
9 under the age of 18 may limit any of the rights pro-
10 vided in this Act.

11 (3) DEFINITIONS.—For purposes of this sub-
12 section:

13 (A) PRE-DISPUTE ARBITRATION AGREE-
14 MENT.—The term “pre-dispute arbitration
15 agreement” means any agreement to arbitrate a
16 dispute that has not arisen at the time of the
17 making of the agreement.

18 (B) PRE-DISPUTE JOINT-ACTION WAIV-
19 ER.—The term “pre-dispute joint-action waiv-
20 er” means an agreement, whether or not part
21 of a pre-dispute arbitration agreement, that
22 would prohibit or waive the right of 1 of the
23 parties to the agreement to participate in a
24 joint, class, or collective action in a judicial, ar-
25 bitral, administrative, or other forum, con-

cerning a dispute that has not yet arisen at the
time of the making of the agreement.

(c) RIGHT TO CURE.—

(1) NOTICE.—Subject to paragraph (3), any action under this section may be brought by an individual if, prior to initiating such action against a covered entity for injunctive relief or against a covered entity that meets the requirements of section 210(c) for any form of relief the individual provides to the covered entity 45 days' written notice identifying the specific provisions of this Act the individual alleges have been or are being violated.

(2) EFFECT OF CURE.—In the event a cure is possible, if within the 45 days the covered entity cures the noticed violation and provides the individual an express written statement that the violation has been cured and that no further violations shall occur, an action for injunctive relief may be reasonably dismissed.

(d) DEMAND LETTER.—If an individual or a class of individuals sends correspondence to a covered entity alleging a violation of the provisions of this Act and requesting a monetary payment, such correspondence shall include the following language: “Please visit the website of the Federal Trade Commission to understand your rights

1 pursuant to this letter” followed by a hyperlink to the web
2 page of the Commission required under section 201. If
3 such correspondence does not include such language and
4 hyperlink, the individual or joint class of individuals shall
5 forfeit their rights under this section.

6 (e) APPLICABILITY.—This section shall only apply to
7 any claim alleging a violation of section 102, 104, 202,
8 203, 204, 205(a), 205(b), 206(c)(3)(D), 207(a), 208(a),
9 or 302 for which relief described in subsection (a)(2) may
10 be granted.

11 **SEC. 404. RELATIONSHIP TO FEDERAL AND STATE LAWS.**

12 (a) FEDERAL LAW PRESERVATION.—

13 (1) IN GENERAL.—Nothing in this Act or a reg-
14 ulation promulgated under this Act shall be con-
15 strued to limit—

16 (A) the authority of the Commission, or
17 any other Executive agency, under any other
18 provision of law;

19 (B) any requirement for a common carrier
20 subject to section 64.2011 of title 47, Code of
21 Federal Regulations, regarding information se-
22 curity breaches; or

23 (C) any other provision of Federal law un-
24 less specifically authorized by this Act.

1 (2) APPLICABILITY OF OTHER PRIVACY RE-
2 QUIREMENTS.—A covered entity that is required to
3 comply with title V of the Gramm-Leach-Bliley Act
4 (15 U.S.C. 6801 et seq.), the Health Information
5 Technology for Economic and Clinical Health Act
6 (42 U.S.C. 17931 et seq.), part C of title XI of the
7 Social Security Act (42 U.S.C. 1320d et seq.), the
8 Fair Credit Reporting Act (15 U.S.C. 1681 et seq.),
9 the Family Educational Rights and Privacy Act (20
10 U.S.C. 1232g; part 99 of title 34, Code of Federal
11 Regulations), or the regulations promulgated pursu-
12 ant to section 264(c) of the Health Insurance Port-
13 ability and Accountability Act of 1996 (42 U.S.C.
14 1320d–2 note), and is in compliance with the data
15 privacy requirements of such regulations, part, title,
16 or Act (as applicable), shall be deemed to be in com-
17 pliance with the related requirements of this title,
18 except for section 208, with respect to data subject
19 to the requirements of such regulations, part, title,
20 or Act. Not later than 1 year after the date of enact-
21 ment of this Act, the Commission shall issue guid-
22 ance describing the implementation of this para-
23 graph.

24 (3) APPLICABILITY OF OTHER DATA SECURITY
25 REQUIREMENTS.—A covered entity that is required

1 to comply with title V of the Gramm-Leach-Bliley
2 Act (15 U.S.C. 6801 et seq.), the Health Informa-
3 tion Technology for Economic and Clinical Health
4 Act (42 U.S.C. 17931 et seq.), part C of title XI of
5 the Social Security Act (42 U.S.C. 1320d et seq.),
6 or the regulations promulgated pursuant to section
7 264(c) of the Health Insurance Portability and Ac-
8 countability Act of 1996 (42 U.S.C. 1320d–2 note),
9 and is in compliance with the information security
10 requirements of such regulations, part, title, or Act
11 (as applicable), shall be deemed to be in compliance
12 with the requirements of section 208 with respect to
13 data subject to the requirements of such regulations,
14 part, title, or Act. Not later than 1 year after the
15 date of enactment of this Act, the Commission shall
16 issue guidance describing the implementation of this
17 paragraph.

18 (b) PREEMPTION OF STATE LAWS.—

19 (1) IN GENERAL.—No State or political subdivi-
20 sion of a State may adopt, maintain, enforce, or con-
21 tinue in effect any law, regulation, rule, standard,
22 requirement, or other provision having the force and
23 effect of law of any State, or political subdivision of
24 a State, covered by the provisions of this Act, or a

1 rule, regulation, or requirement promulgated under
2 this Act.

3 (2) STATE LAW PRESERVATION.—Paragraph
4 (1) shall not be construed to preempt, displace, or
5 supplant the following State laws, rules, regulations,
6 or requirements:

7 (A) Consumer protection laws of general
8 applicability such as laws regulating deceptive,
9 unfair, or unconscionable practices.

10 (B) Civil rights laws.

11 (C) Laws that govern the privacy rights or
12 other protections of employees, employee infor-
13 mation, students, or student information.

14 (D) Laws that address notification require-
15 ments in the event of a data breach.

16 (E) Contract or tort law.

17 (F) Criminal laws governing fraud, theft,
18 including identity theft, unauthorized access to
19 information or electronic devices, or unauthor-
20 ized use of information, malicious behavior, or
21 similar provisions, or laws of criminal proce-
22 dure.

23 (G) Criminal or civil laws regarding
24 cyberstalking, cyberbullying, nonconsensual por-
25 nography, or sexual harassment.

1 (H) Public safety or sector specific laws
2 unrelated to privacy or security.

3 (I) Laws that address public records,
4 criminal justice information systems, arrest
5 records, mug shots, conviction records, or non-
6 conviction records.

7 (J) Laws that address banking records, fi-
8 nancial records, tax records, Social Security
9 numbers, credit cards, credit reporting and in-
10 vestigations, credit repair, credit clinics, or
11 check-cashing services.

12 (K) Laws that solely address facial rec-
13 ognition or facial recognition technologies, elec-
14 tronic surveillance, wiretapping, or telephone
15 monitoring.

16 (L) The Biometric Information Privacy
17 Act (740 ICLS 14 et seq.) and the Genetic In-
18 formation Privacy Act (410 ILCS et seq.).

19 (M) Laws to address unsolicited email
20 messages, telephone solicitation, or caller ID.

21 (N) Laws that address health information,
22 medical information, medical records, HIV sta-
23 tus, or HIV testing.

24 (O) Laws that address the confidentiality
25 of library records.

1 (P) Section 1798.150 of the California
2 Civil Code (as amended on November 3, 2020,
3 by initiative Proposition 24, section 16).

4 (3) NONAPPLICATION OF FCC PRIVACY LAWS
5 AND REGULATIONS TO COVERED ENTITIES.—Not-
6 withstanding any other provision of law, sections
7 222, 338(i), and 631 of the Communications Act of
8 1934, as amended (47 U.S.C. 222, 338(i), and 551),
9 and any regulation promulgated by the Federal
10 Communications Commission under such sections,
11 shall not apply to any covered entity with respect to
12 the collecting, processing, or transferring of covered
13 data under this Act.

14 (c) PRESERVATION OF COMMON LAW OR STATUTORY
15 CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this
16 Act, nor any amendment, standard, rule, requirement, as-
17 sessment, law, or regulation promulgated under this Act,
18 shall be construed to preempt, displace, or supplant any
19 Federal or State common law rights or remedies, or any
20 statute creating a remedy for civil relief, including any
21 cause of action for personal injury, wrongful death, prop-
22 erty damage, or other financial, physical, reputational, or
23 psychological injury based in negligence, strict liability,
24 products liability, failure to warn, an objectively offensive
25 intrusion into the private affairs or concerns of the indi-

1 vidual, or any other legal theory of liability under any Fed-
2 eral or State common law, or any State statutory law, ex-
3 cept that the fact of a violation of this Act shall not be
4 pleaded as an element of any such cause of action.

5 **SEC. 405. SEVERABILITY.**

6 If any provision of this Act, or the application thereof
7 to any person or circumstance, is held invalid, the remain-
8 der of this Act and the application of such provision to
9 other persons not similarly situated or to other cir-
10 cumstances shall not be affected by the invalidation.

11 **SEC. 406. COPPA.**

12 (a) IN GENERAL.—Nothing in this Act shall be con-
13 strued to relieve or change any obligations that a covered
14 entity or another person may have under the Children’s
15 Online Privacy Protection Act of 1998 (15 U.S.C. 6501
16 et seq.).

17 (b) UPDATED REGULATIONS.—Not later than 180
18 days after the enactment of this Act, the Commission shall
19 amend its rules issued pursuant to the Children’s Online
20 Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.)
21 to make reference to the additional requirements placed
22 on covered entities under this Act, in addition to those
23 already enacted under the Children’s Online Privacy Pro-
24 tection Act of 1998 that may already apply to some of
25 such covered entities.

1 **SEC. 407. AUTHORIZATION OF APPROPRIATIONS.**

2 There are authorized to be appropriated to the Com-
3 mission such sums as necessary to carry out this Act.

4 **SEC. 408. EFFECTIVE DATE.**

5 Except as otherwise provided, this Act shall take ef-
6 fect on the date that is 180 days after the date of enact-
7 ment of this Act.

